

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK			
First Named Inventor/Applicant Name:	Victor LARSON, et al.			
Filer:	William Neal Hughet/Tamika Miles			
Attorney Docket Number:	3755-121			
Filed as Large Entity				
inter partes reexam Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Request for inter reexamination	1813	1	8800	8800
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				8800

Electronic Acknowledgement Receipt

EFS ID:	6519927
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor LARSON, et al.
Customer Number:	06449
Filer:	William Neal Hughet/Tamika Miles
Filer Authorized By:	William Neal Hughet
Attorney Docket Number:	3755-121
Receipt Date:	25-NOV-2009
Filing Date:	
Time Stamp:	17:51:00
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$8800
RAM confirmation Number	3597
Deposit Account	022135
Authorized User	

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	NPL Documents	Exhibit1Larson.pdf	4244893	no	74
			9b62e67b2e288c2444923b8b039cdb5dcd979e58		
Warnings:					
Information:					
2	NPL Documents	Exhibit2AventailConnectAdmin Guide31.pdf	622865	no	125
			8e07ec55b404a1379f3b321717a6b32c242b273f		
Warnings:					
Information:					
3	NPL Documents	Exhibit3VirtualPrivateNetworkingAnOverview.pdf	1149224	no	28
			0242245ead3aa2adffd6065473a68b1e7e7a9cca		
Warnings:					
Information:					
4	NPL Documents	Exhibit4RFC1035.pdf	98259	no	56
			13c7f89f3ac478d680feedbb39ca193a76be09d4		
Warnings:					
Information:					
5	NPL Documents	Exhibit7GalvinPublicKeyDistributionwithSecure.pdf	956965	no	12
			602f424067b8e2f6fa24f9a84d6b36277b050998		
Warnings:					
Information:					
6	NPL Documents	Exhibit8aGauntletFirewallforWindowsNTAdmin.pdf	21350755	no	138
			603d7d4e94e2fb6cd62cf72a521c1fc31be05f2d		
Warnings:					
Information:					
7	NPL Documents	Exhibit10InstallingConfiguring andUsingPPTP.pdf	2428789	no	30
			ed4fda47a68b292551ea9be20fc23c12a55b7784		
Warnings:					
Information:					
8	NPL Documents	Exhibit11BuildingaMicrosoftVPNAComprehensiveCollection.pdf	23764386	no	216
			09d54486aaf273a32e9a700eccd0c3ae32cb363ed		

Warnings:					
Information:					
9	NPL Documents	Exhibit14NoticeofAllowance486.pdf	438608 a0a9aa7f4202dbb95770dc7e16f9bfae62811314	no	10
Warnings:					
Information:					
10	NPL Documents	Exhibit9.pdf	8264306 52ce8cb87ca2651a9426c80c16cb85c60a331563	no	106
Warnings:					
Information:					
11	NPL Documents	Exhibit8bGauntletFirewallforWindowsNTAdmin.pdf	19719372 9d900a7358c6551b568daffbeb0db739564c8011	no	139
Warnings:					
Information:					
12	NPL Documents	Exhibit5BuildingaMicrosoftVPN.pdf	23778793 6cfa308964b9f93791ddb9b56a53878ced63d677	no	216
Warnings:					
Information:					
13	NPL Documents	Exhibit5KosiorBuildingandManagingVPNs2.pdf	11662304 04d8a5135bc2b9440b32190ce3600517b9a307b8	no	180
Warnings:					
Information:					
14	NPL Documents	Exhibit6KaufmanImplementingIPsec1.pdf	14401558 11d6f856b09bdf26a55c1c03c51632d04b2584d7	no	200
Warnings:					
Information:					
15	NPL Documents	Exhibit6KaufmanImplementingIPsec2.pdf	10427650 7553db79ae8104dab359c5c50a32123139c541f1	no	80
Warnings:					
Information:					
16	NPL Documents	Exhibit12SBO8.pdf	296349 14ddd8219880566aaa1ead7ef64067252808a0db	no	5
Warnings:					
Information:					
17	NPL Documents	Exhibit13ClaimConstructionOrder.pdf	3809824 e1502e14d91261820fd2e8abf322fbc320ea2384	no	36

Warnings:					
Information:					
18	NPL Documents	AppA180ClaimChartAventail.pdf	3372015 a81cf8bd089146dc2a198a36fc6b378e485b5480	no	37
Warnings:					
Information:					
19	NPL Documents	AppB180ClaimChartVPNOverviewRFC1035.pdf	3070716 3e4bf5fc7c25442ed9858cad77fba3364bac5b0	no	38
Warnings:					
Information:					
20	NPL Documents	AppC180ClaimChartKosior.pdf	2040813 b96ea6cdf6f8fee18b487b60b45a06f25e61338a	no	24
Warnings:					
Information:					
21	NPL Documents	AppD180ClaimChartKaufman.pdf	2284985 c66841f9c4134e7d4834be3032bfe53e891c3f3c	no	24
Warnings:					
Information:					
22	NPL Documents	AppE180ClaimChartKaufmanGalvin.pdf	2350205 d78a6d5d1d3b4d63580725599f0e0280d9e271b1	no	35
Warnings:					
Information:					
23	NPL Documents	AppF180ClaimChartGauntlet.pdf	2046277 d4de413ae130c4409bbd38a53f032ec618847ff3	no	31
Warnings:					
Information:					
24	NPL Documents	AppG180ClaimChartHandsOnInstallingNT.pdf	2561466 190f81e55c88275583da851e32bdc43211611aad	no	23
Warnings:					
Information:					
25	NPL Documents	AppH180ClaimChartMicrosoftVPN.pdf	872923 211f7dcf3a676256c78881238103cd1c99178654	no	20
Warnings:					
Information:					
26	Receipt of Original Inter Partes Reexam Request	Reqforreexam180patent.pdf	6348049 84f78dac47c46e549991a7ed096ec7a925cb14a9	no	53

Warnings:					
Information:					
27	Miscellaneous Incoming Letter	121CertificateofServices.pdf	150623 74c37d117c3d17145d9986ced73a8cfb85079985	no	3
Warnings:					
Information:					
28	Fee Worksheet (PTO-875)	fee-info.pdf	30065 f864f7395f4d4825244f74b6b6a8070b905ad6f2	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			172543037		
<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>					

Request for Reexamination of 7,188,180

Exhibit 1

U.S. Patent No. 7,188,180



US007188180B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.:** **US 7,188,180 B2**
(45) **Date of Patent:** **Mar. 6, 2007**

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

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Durham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VimetX, Inc.**, Scotts Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 413 days.

(21) Appl. No.: **10/702,486**

(22) Filed: **Nov. 7, 2003**

(65) **Prior Publication Data**
US 2004/0107285 A1 Jun. 3, 2004

Related U.S. Application Data

(60) Division of application No. 09/558,209, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/137,704, filed on Jun. 7, 1999, provisional application No. 60/106,261, filed on Oct. 30, 1998.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/227; 709/228**

(58) **Field of Classification Search** **709/225-229, 709/245**

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.
5,341,426 A 8/1994 Barney et al.
5,588,060 A 12/1996 Aziz
5,689,566 A 11/1997 Nguyen

(Continued)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Jun. 18, 2002), International Application No. PCT/US01/13260.

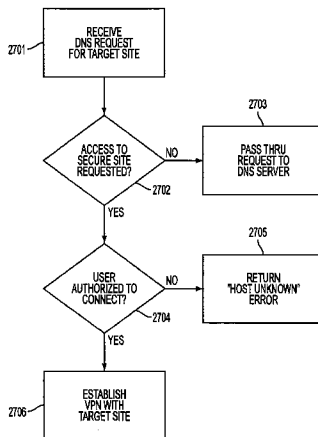
(Continued)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witcoff, Ltd.

(57) **ABSTRACT**

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

41 Claims, 40 Drawing Sheets



U.S. PATENT DOCUMENTS

5,787,172	A	7/1998	Arnold	
5,796,942	A	8/1998	Esbensen	
5,805,801	A	9/1998	Holloway et al.	
5,842,040	A	11/1998	Hughes et al.	
5,870,610	A	2/1999	Beyda et al.	
5,878,231	A	3/1999	Baehr et al.	
5,892,903	A	4/1999	Klaus	
5,898,830	A	4/1999	Wesinger, Jr. et al.	
5,905,859	A	5/1999	Holloway et al.	
6,006,259	A	12/1999	Adelman et al.	
6,016,318	A	1/2000	Tomoiike	
6,052,788	A	4/2000	Wesinger, Jr. et al.	
6,079,020	A	6/2000	Liu	
6,092,200	A	7/2000	Muniyappa et al.	
6,119,171	A *	9/2000	Alkhatib	709/245
6,119,234	A *	9/2000	Aziz et al.	726/11
6,158,011	A	12/2000	Chen et al.	
6,178,409	B1	1/2001	Weber et al.	
6,178,505	B1	1/2001	Schneider et al.	
6,226,751	B1	5/2001	Arrow et al.	
6,243,749	B1	6/2001	Sitaraman et al.	
6,256,671	B1 *	7/2001	Strentzsch et al.	709/227
6,286,047	B1	9/2001	Ramanathan et al.	
6,330,562	B1	12/2001	Boden et al.	
6,332,158	B1	12/2001	Risley et al.	
6,353,614	B1	3/2002	Borella et al.	

FOREIGN PATENT DOCUMENTS

EP	0 814 589	12/1997
EP	0 814 589 A	12/1997
EP	0 838 930	4/1998
EP	0 838 930 A	4/1998
EP	0 858 189	8/1998
GB	2 317 792	4/1998
GB	2 317 792 A	4/1998
GB	2 334 181 A	8/1999
WO	9827783 A	6/1998
WO	WO 98/27783	6/1998
WO	WO 98 55930	12/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Search Report (dated Jun. 28, 2002), International Application No. PCT/US01/13261.
 Donald E. Eastlake, "Domain Name System Security Extensions", DNS Security Working Group, Apr. 1998, 51 pages.
 D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-297 and pp. 351-375.
 P. Srisuresh et al., "DNS extensions to Network Address Translators", Jul. 1998, 27 pages.
 Laurie Wells, "Security Icon", Oct. 19, 1998, 1 page.
 W. Stallings, "Cryptography And Network Security", 2nd Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.

W. Stallings, "New Cryptography and Network Security Book", Jun. 8, 1998, 3 pages.
 Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE publication, 1996, pp. 963-967.
 Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.
 Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.
 Shree Murthy et al., "Congestion-Oriented Shortest Multipath Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.
 Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.
 James E. Bellaire, "New Statement of Rules—Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.
 D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.
 August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.
 Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.
 Linux FreeS/WAN Index File, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/on Feb. 21, 2002, 3 Pages.
 J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.
 Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/glossary.html on Feb. 21, 2002, 25 pages.
 Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from <http://www.netscape.com/eng/ssl3/draft302.txt> on Feb. 4, 2002, 56 pages.
 Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.
 F. Halsall, "Data Communications, Computer Networks And Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.
 Reiter, Michael K. and Rubin, Aviel D. (AI&T Labs—Research), "Crowds: Anonymity for Web Transmission", pp. 1-23.
 Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.
 Rubin, Aviel D., Greer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.
 Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.
 Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606.
 Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Workshop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-66695-B, retrieved from the Internet: URL: <http://www.springerlink.com/content/4uac0tb0hecoma89/fulltext.pdf> (Abstract).

* cited by examiner

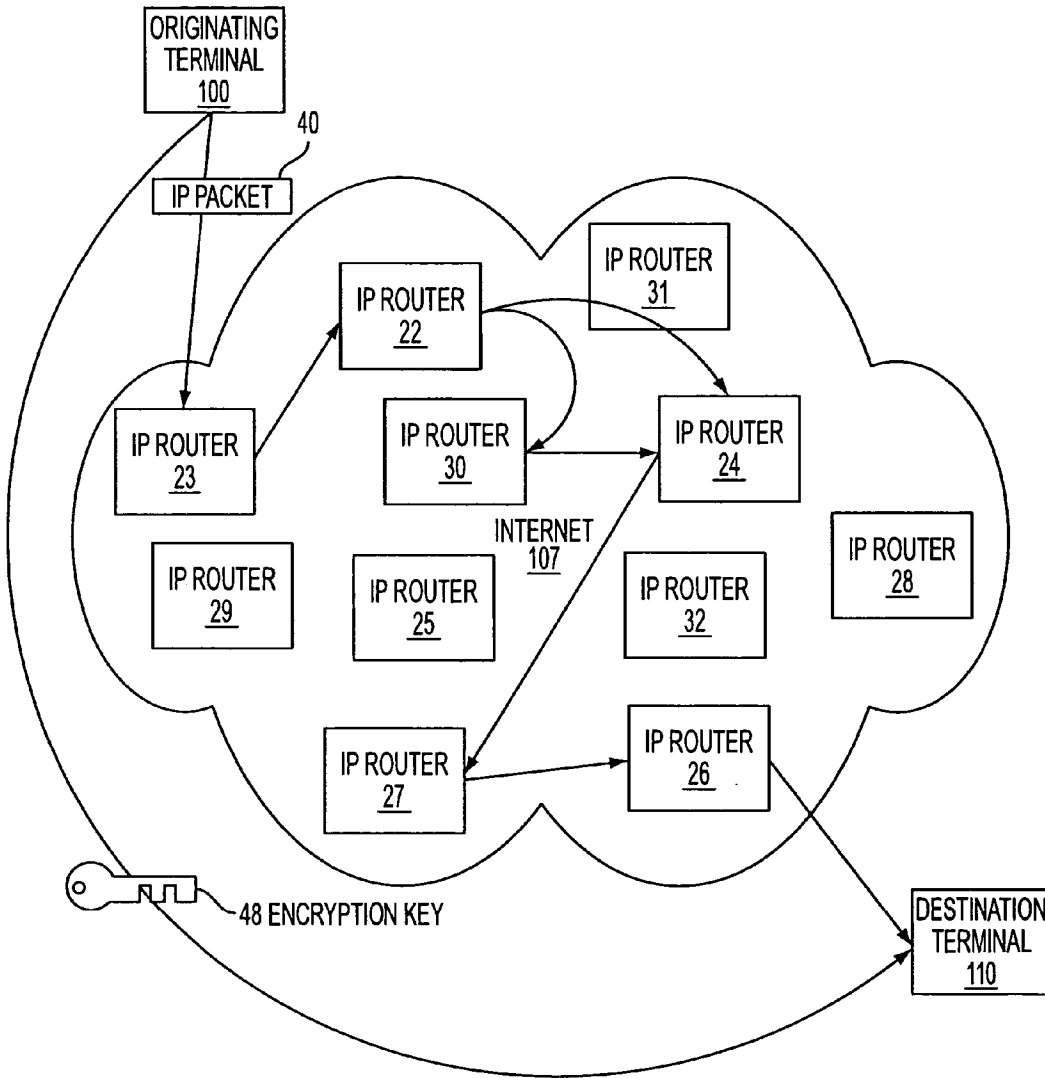


FIG. 1

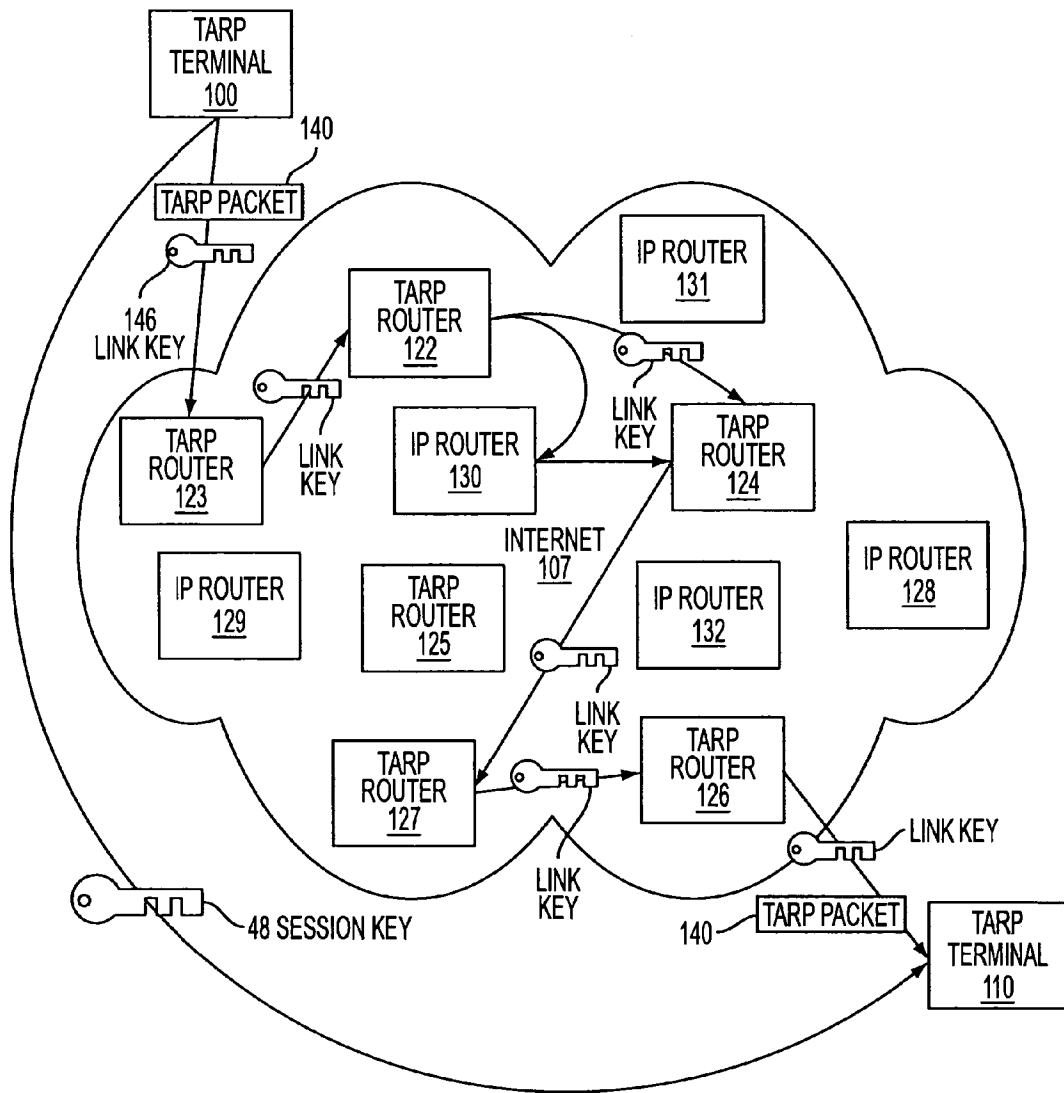


FIG. 2

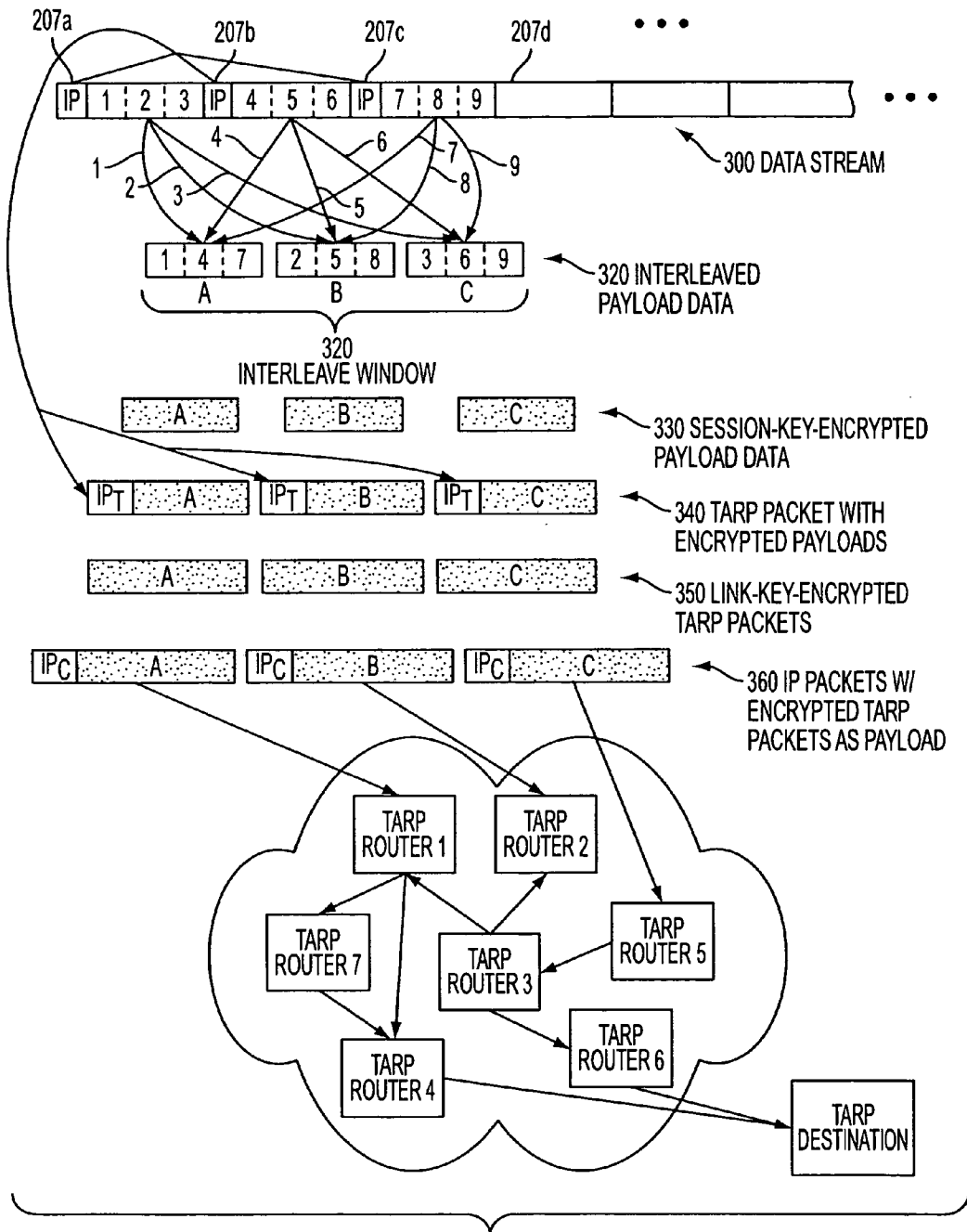


FIG. 3A

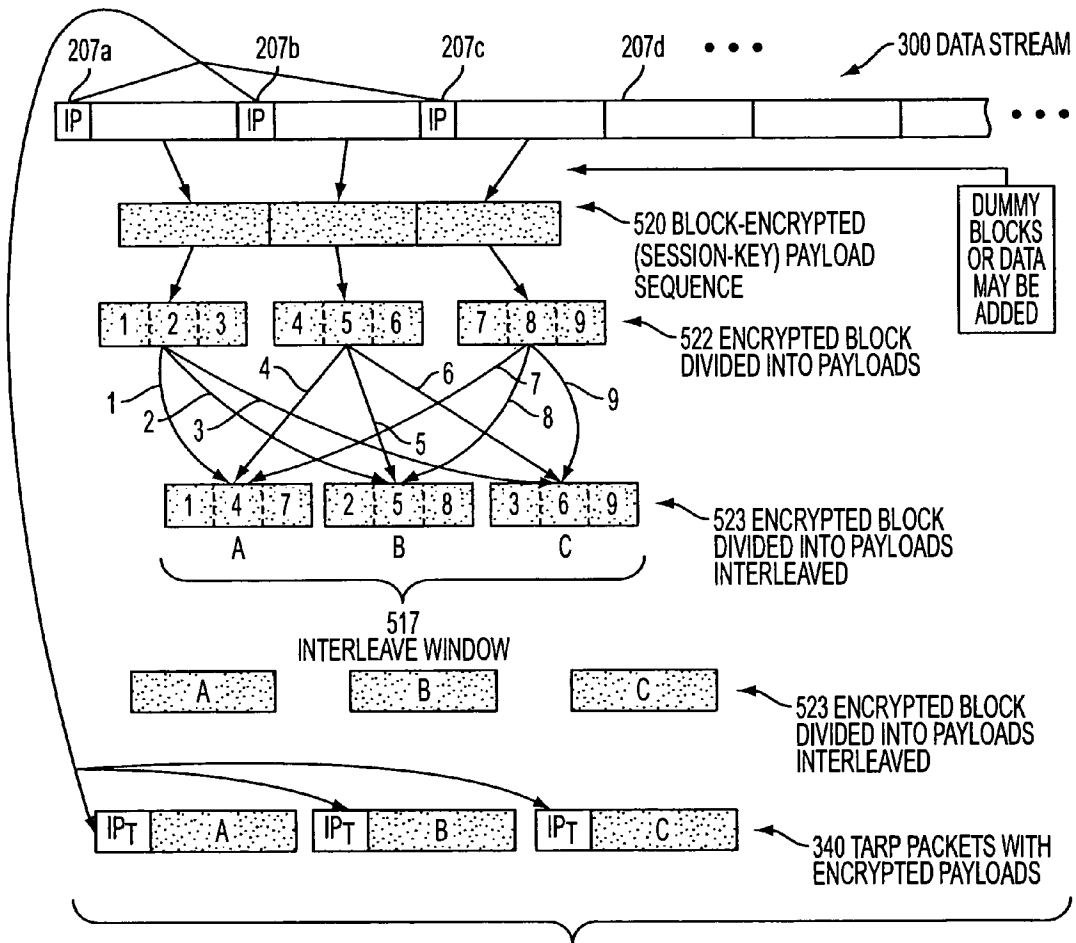


FIG. 3B

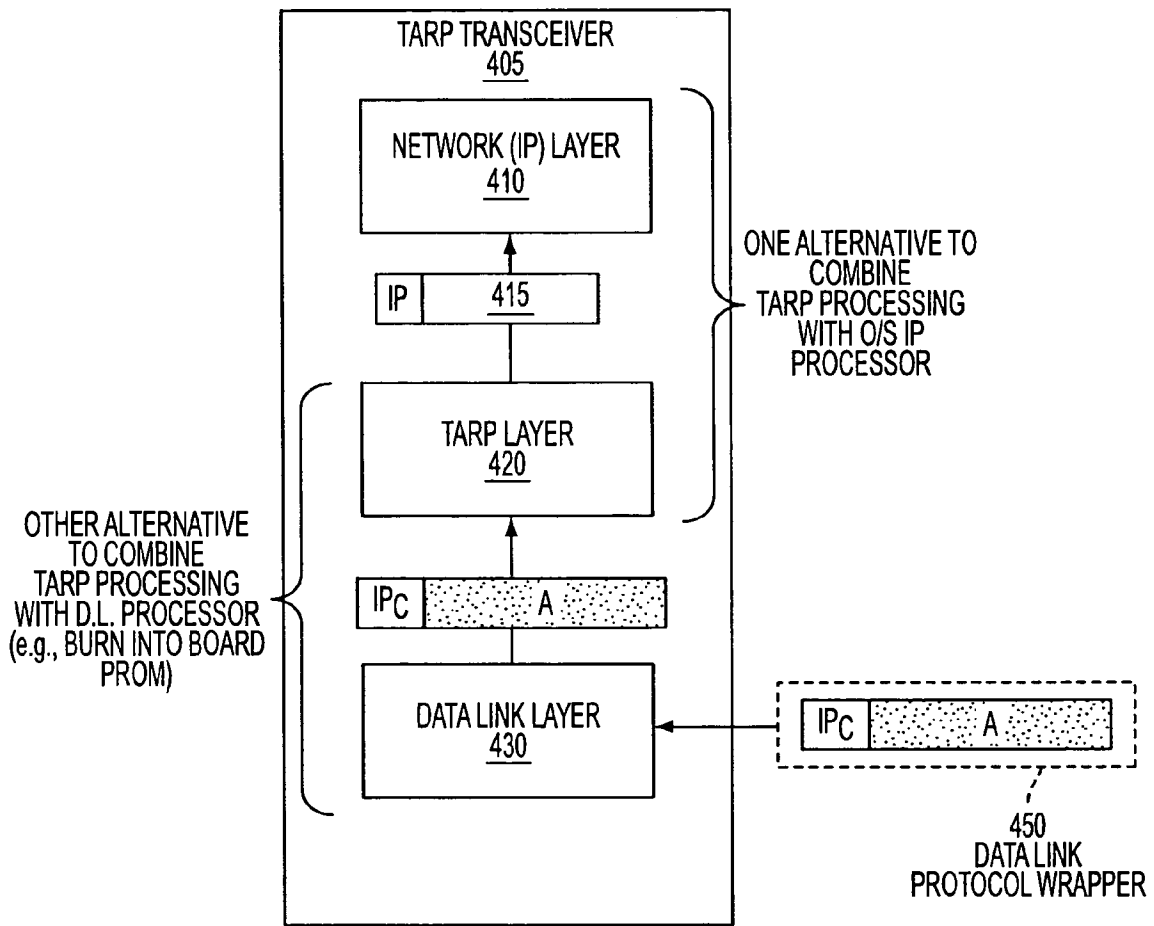


FIG. 4

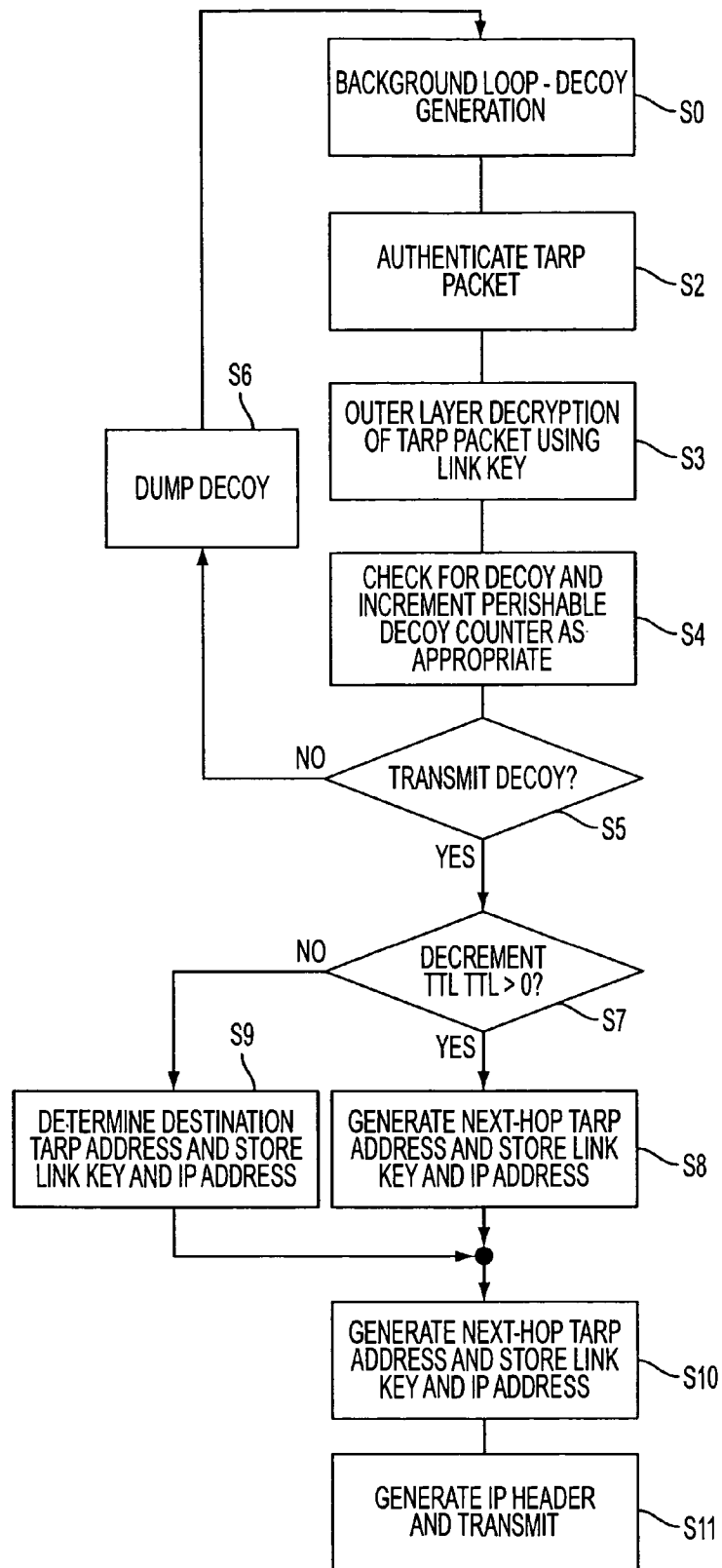


FIG. 5

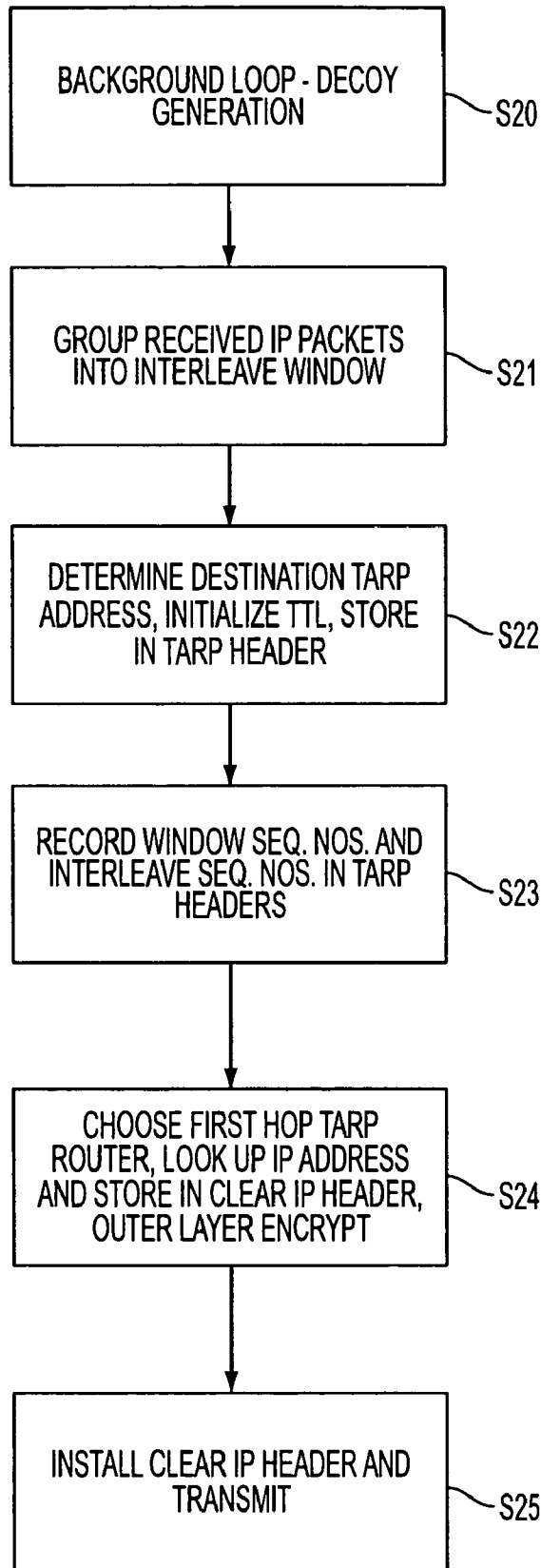


FIG. 6

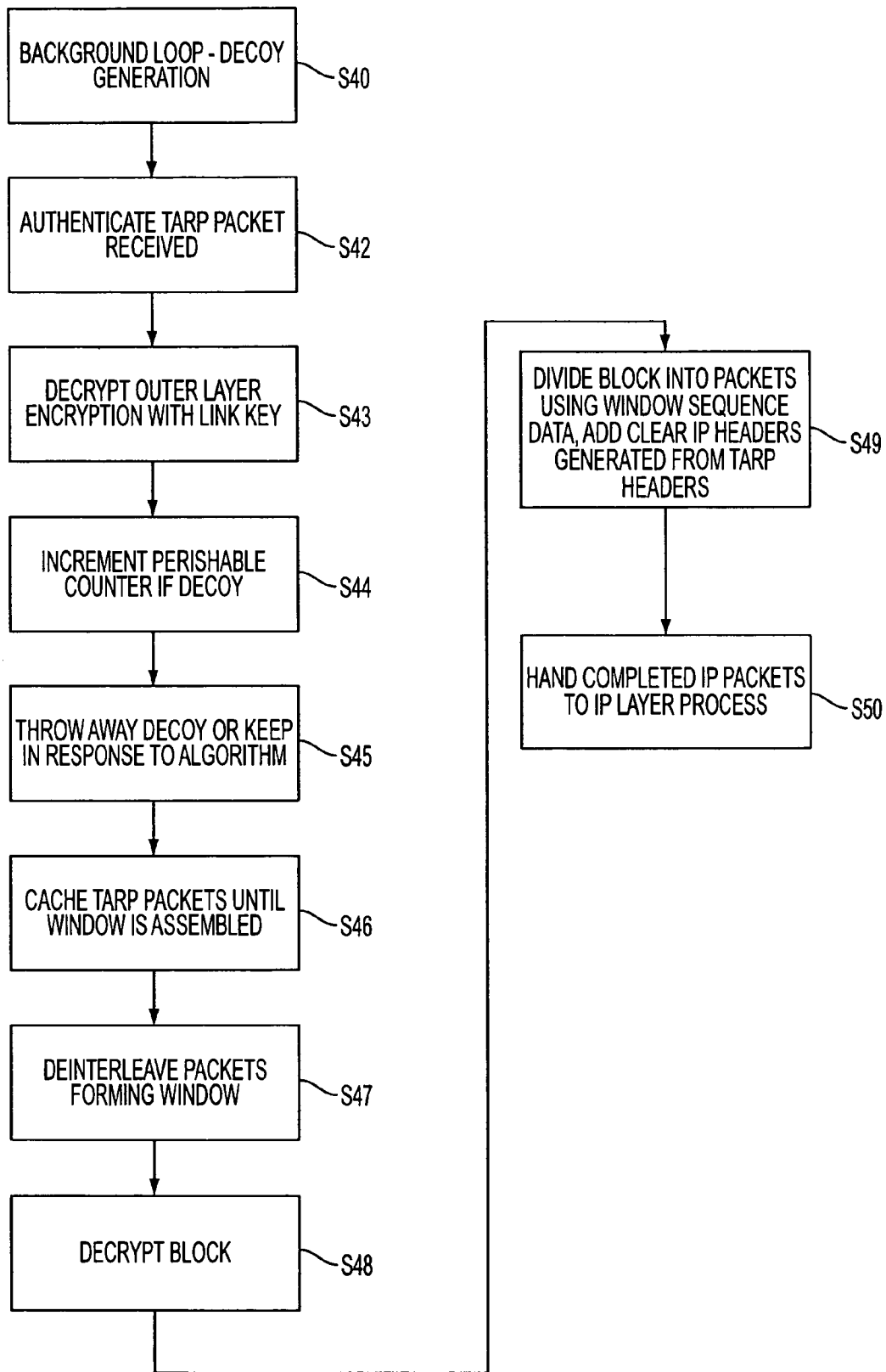


FIG. 7

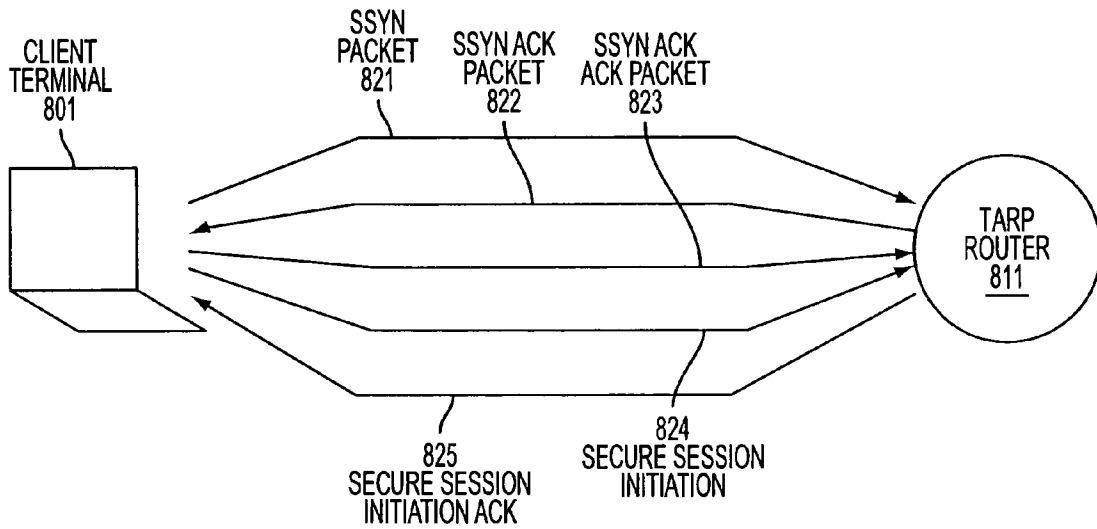


FIG. 8

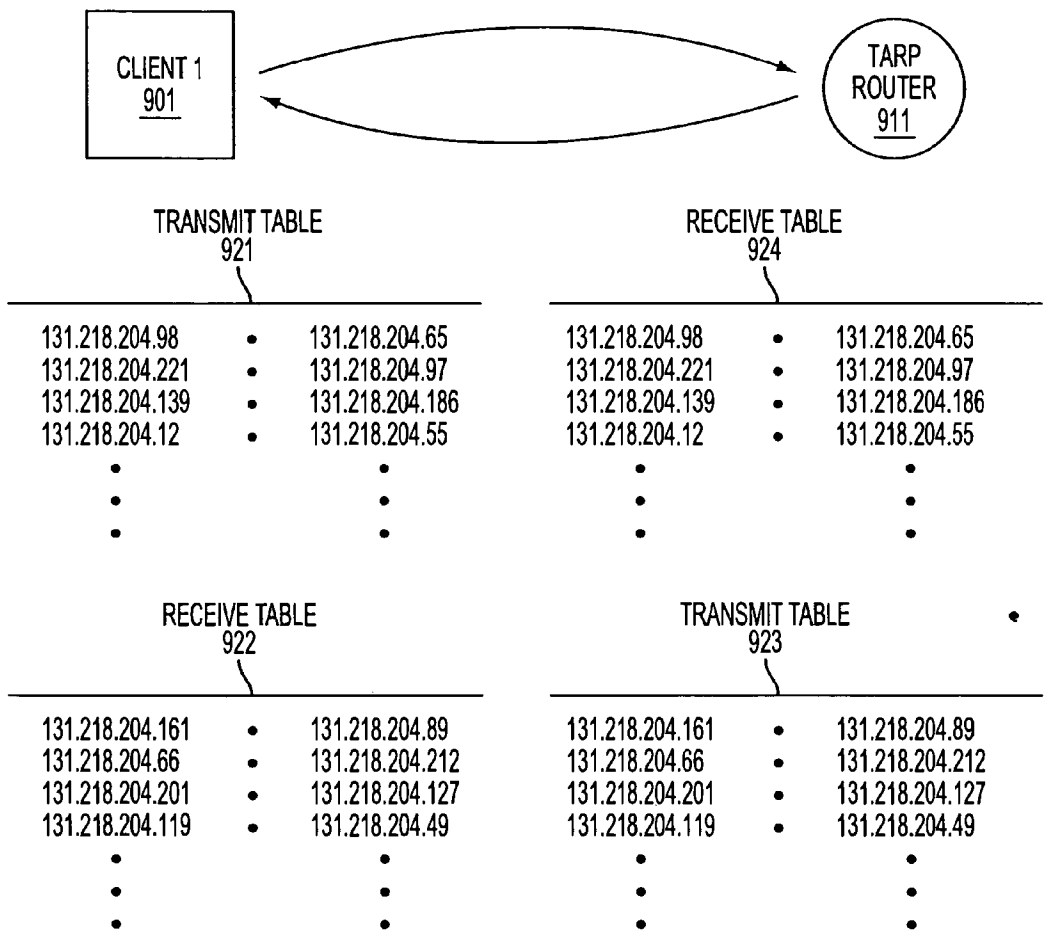


FIG. 9

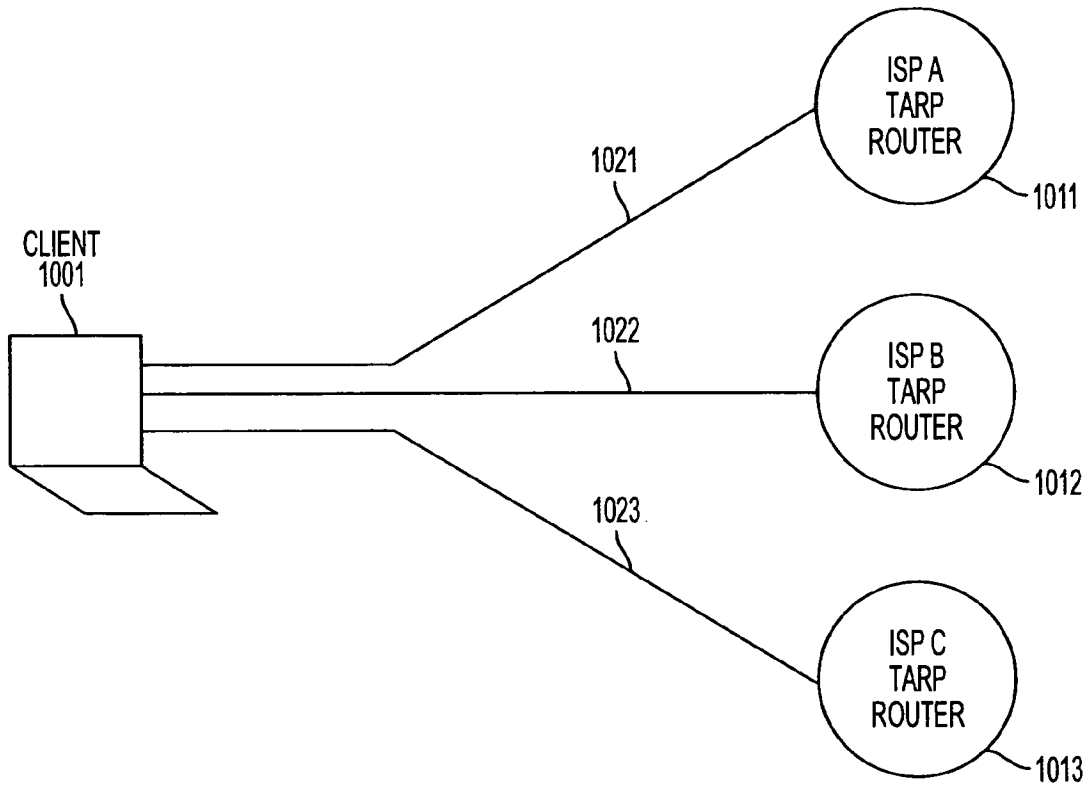


FIG. 10

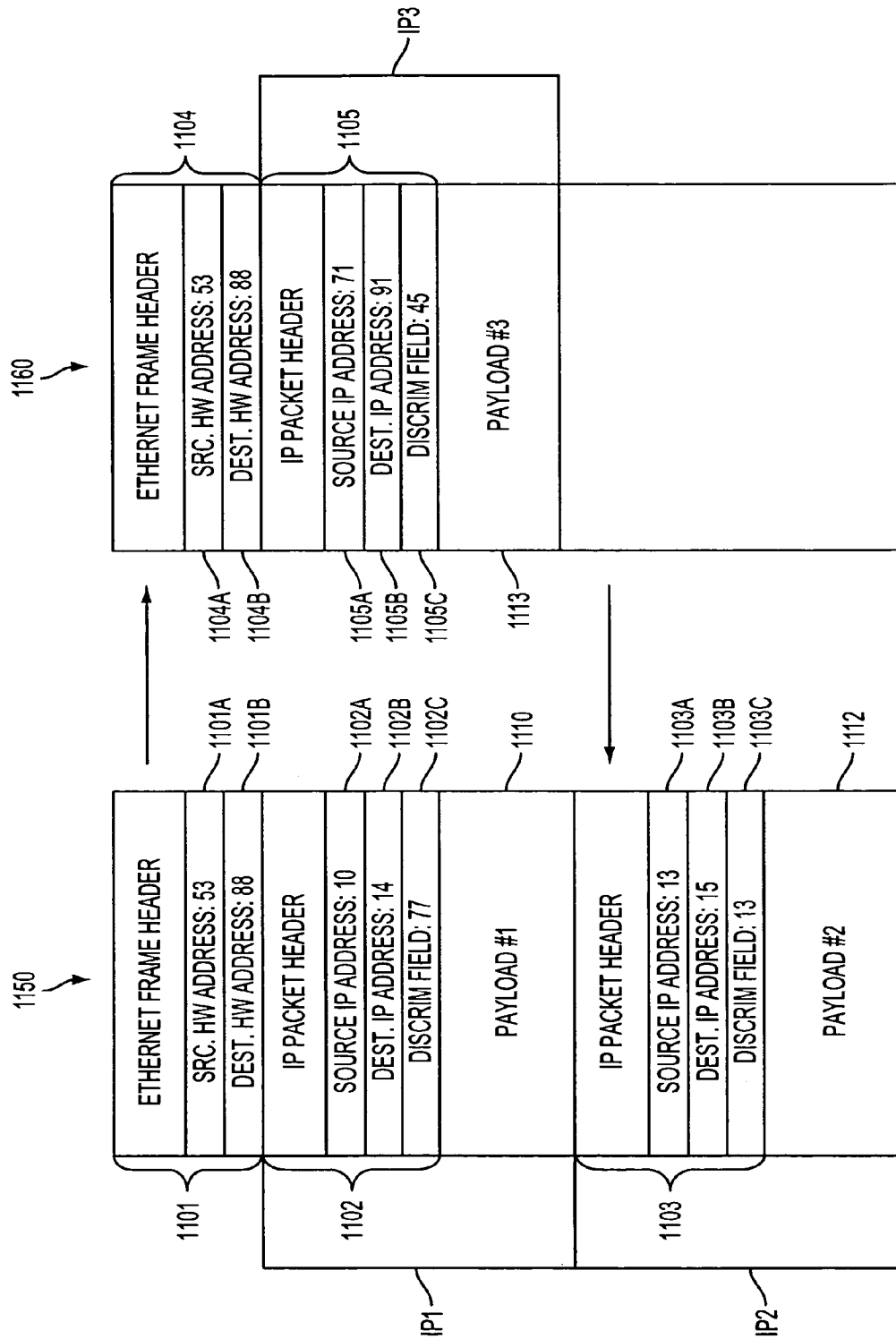


FIG. 11

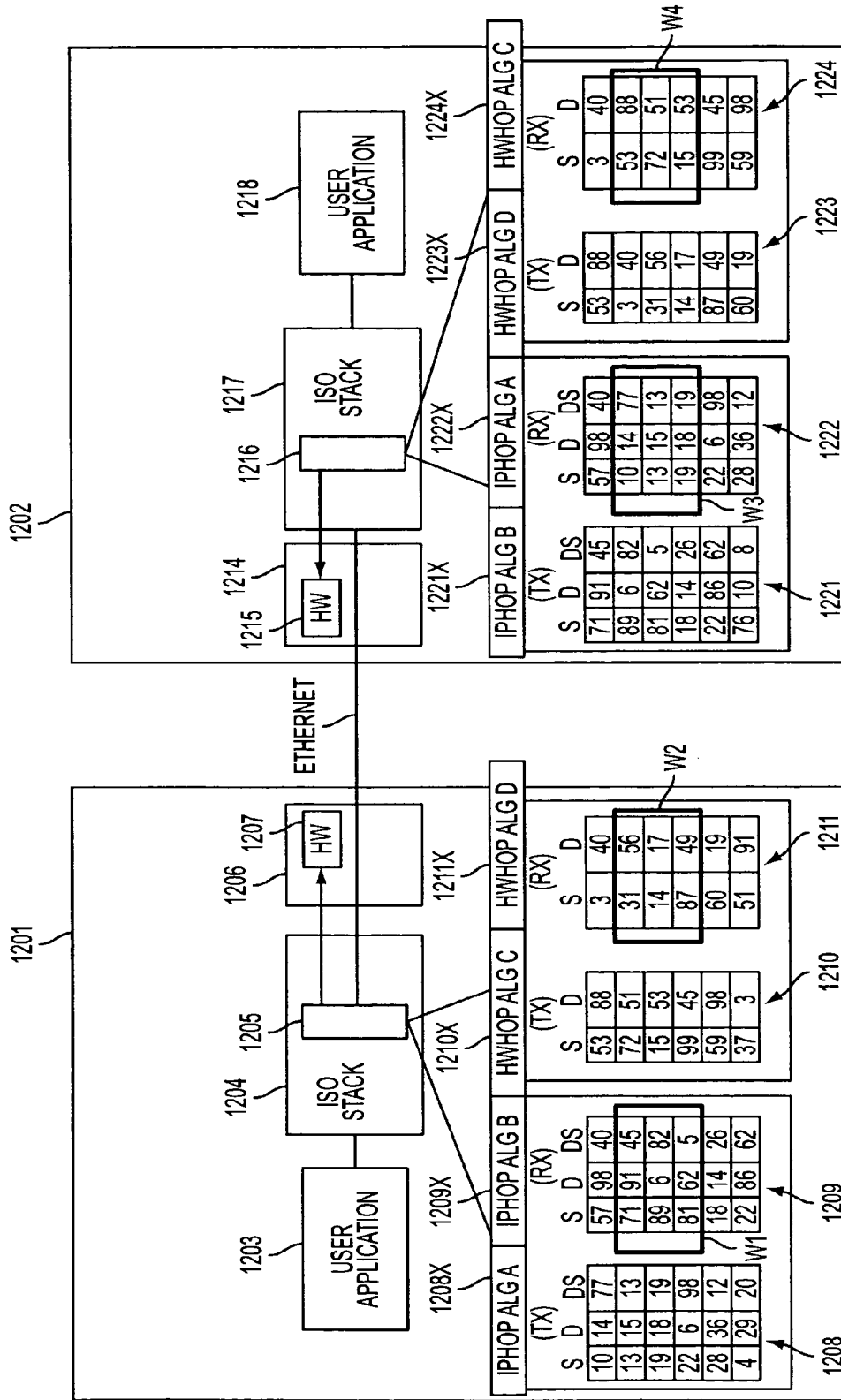


FIG. 12A

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

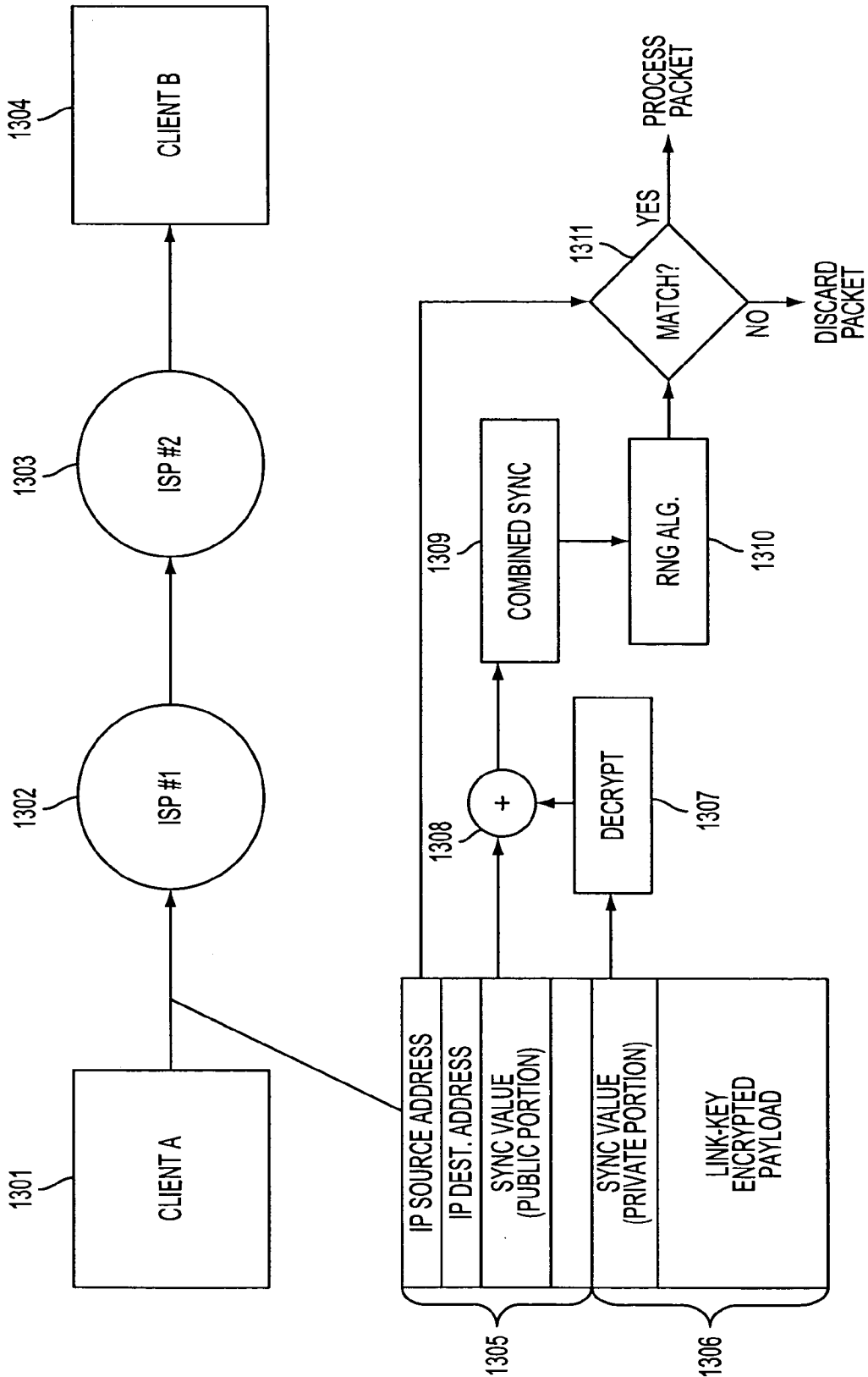


FIG. 13

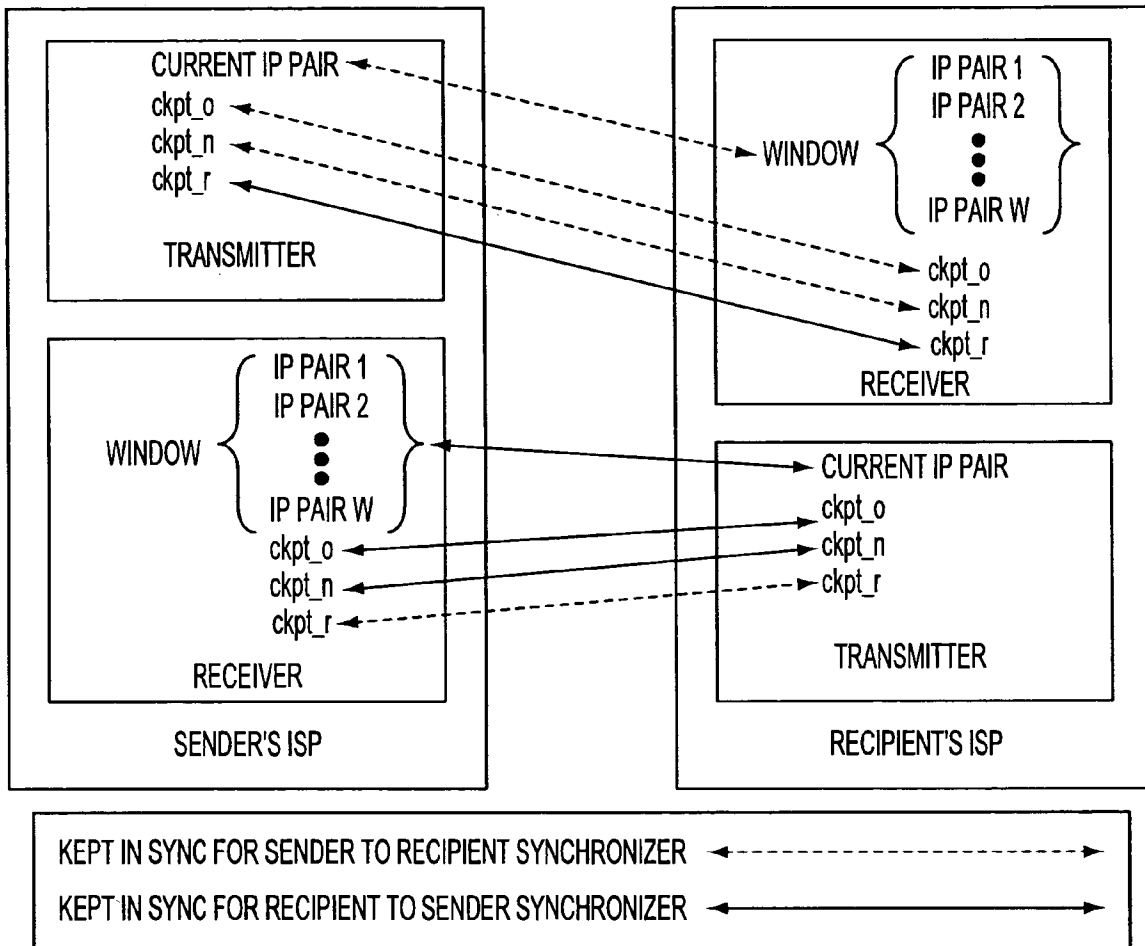


FIG. 14

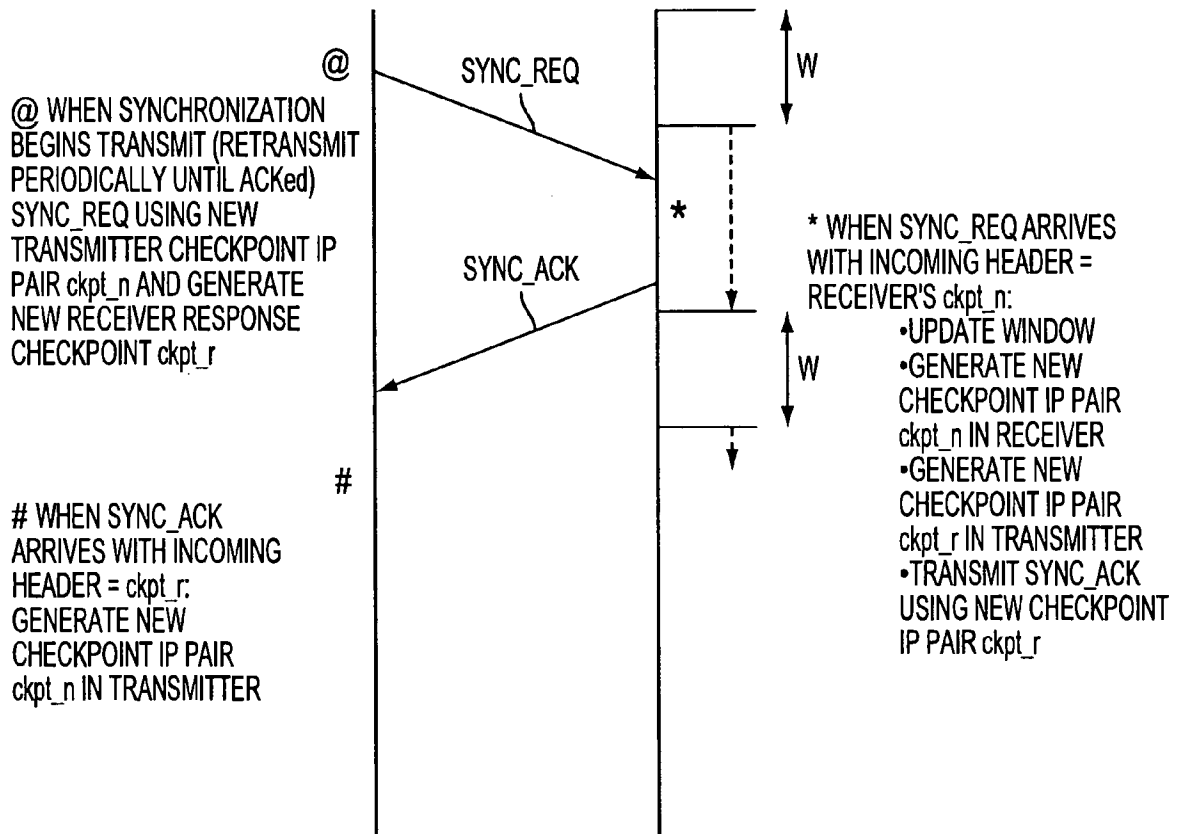


FIG. 15

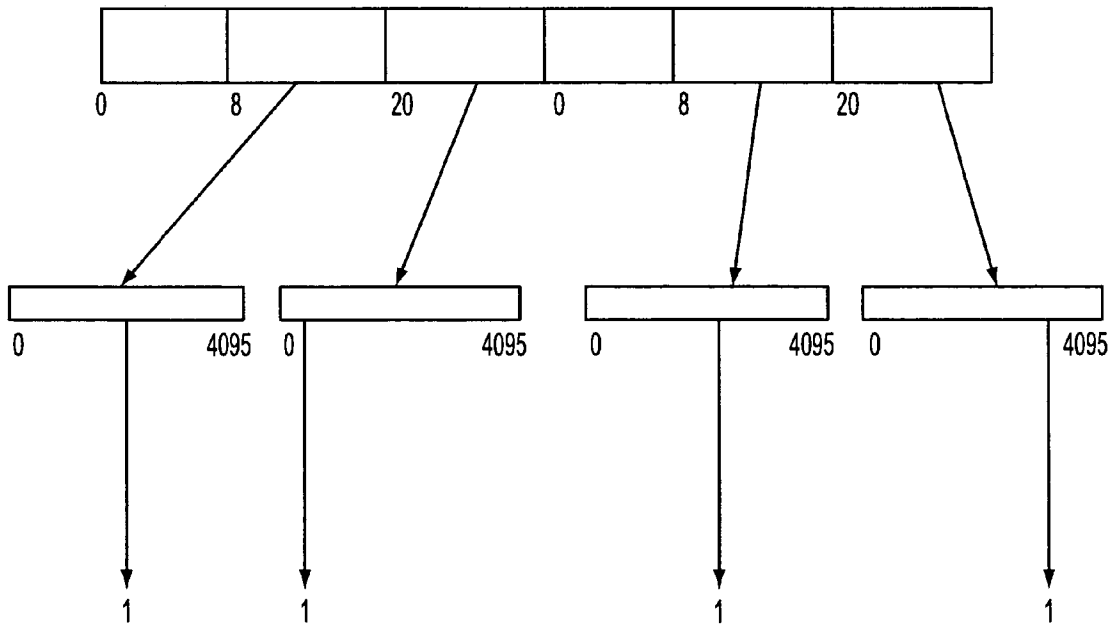


FIG. 16

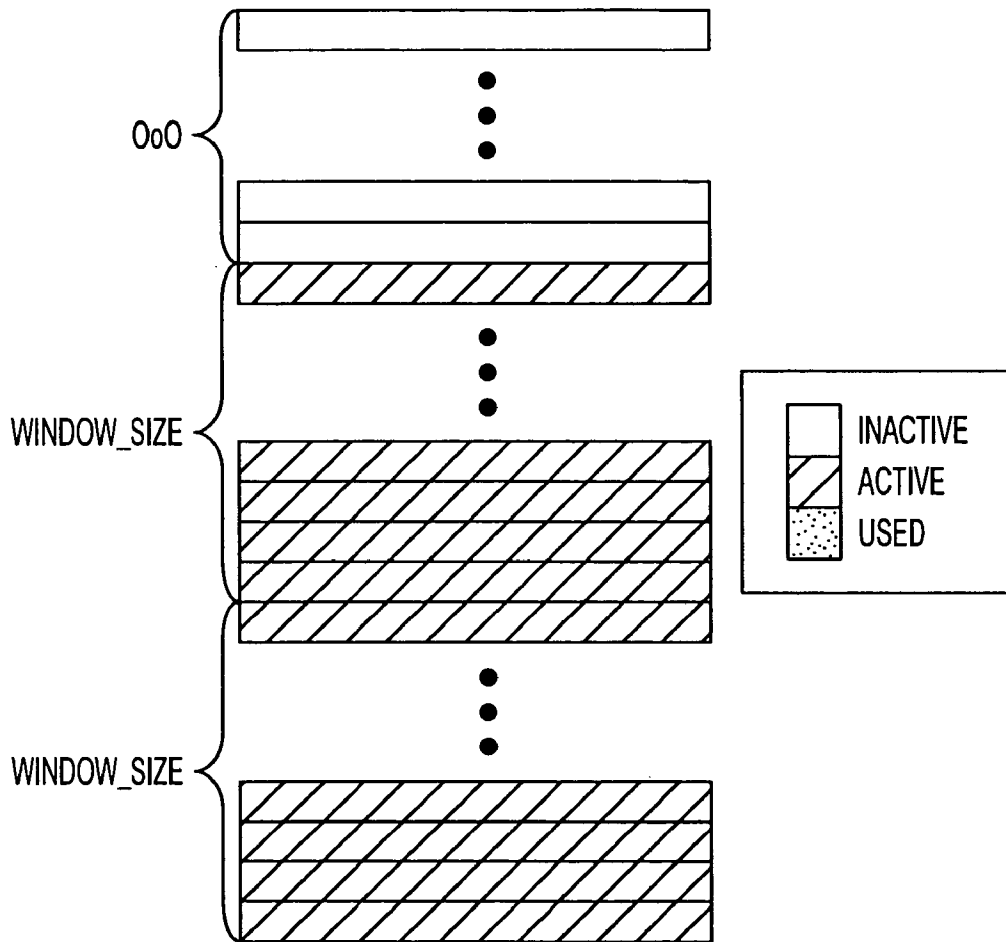


FIG. 17

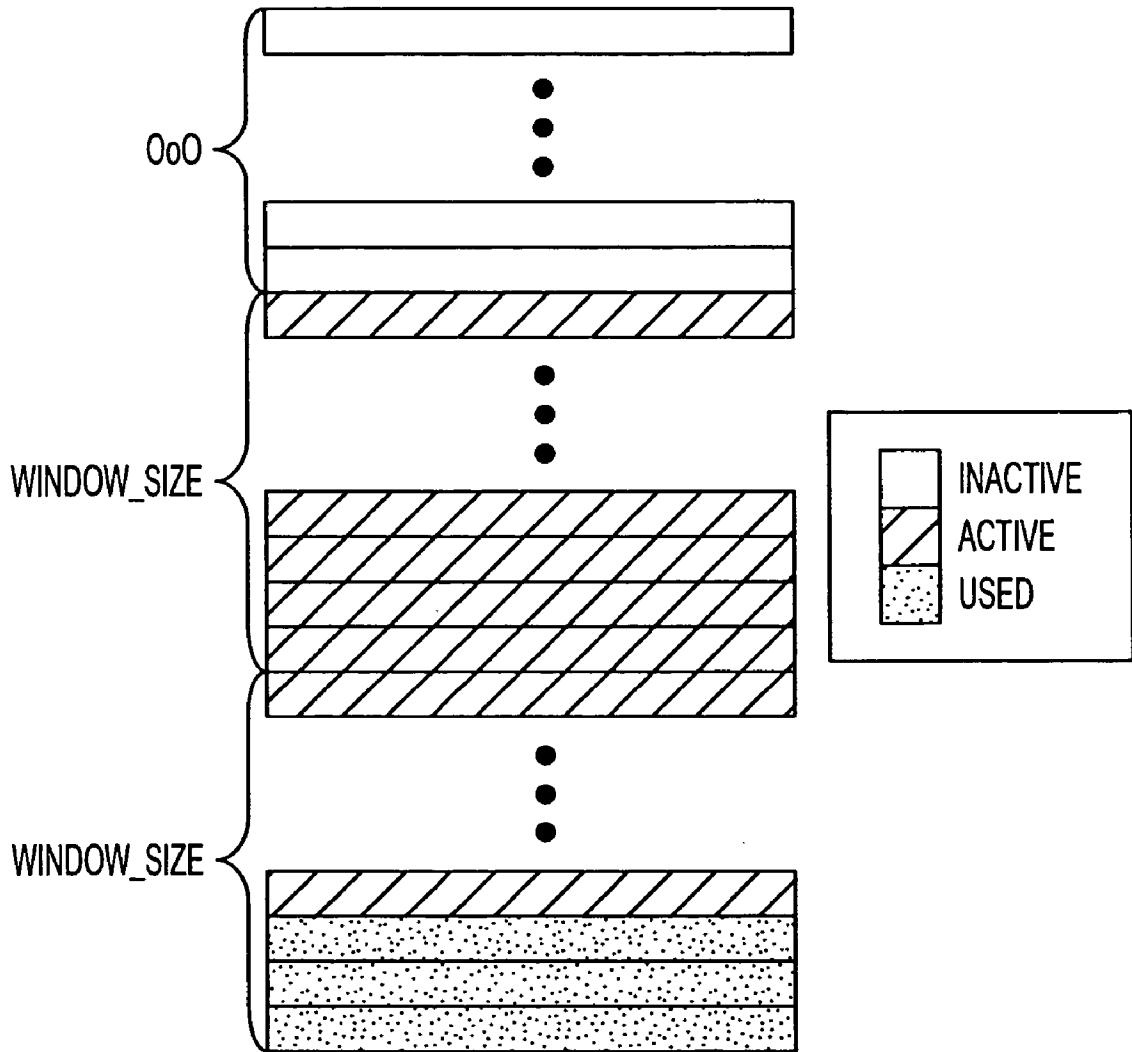


FIG. 18

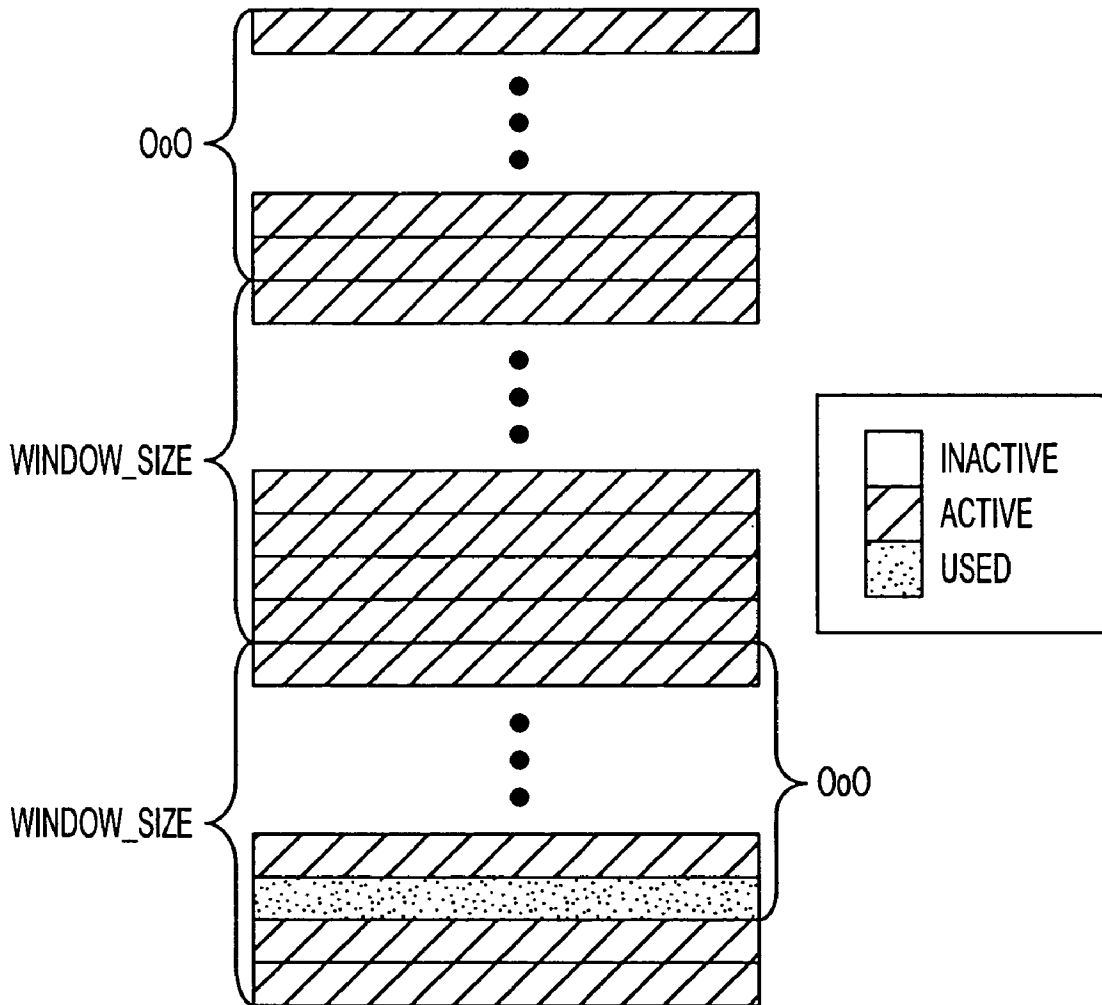


FIG. 19

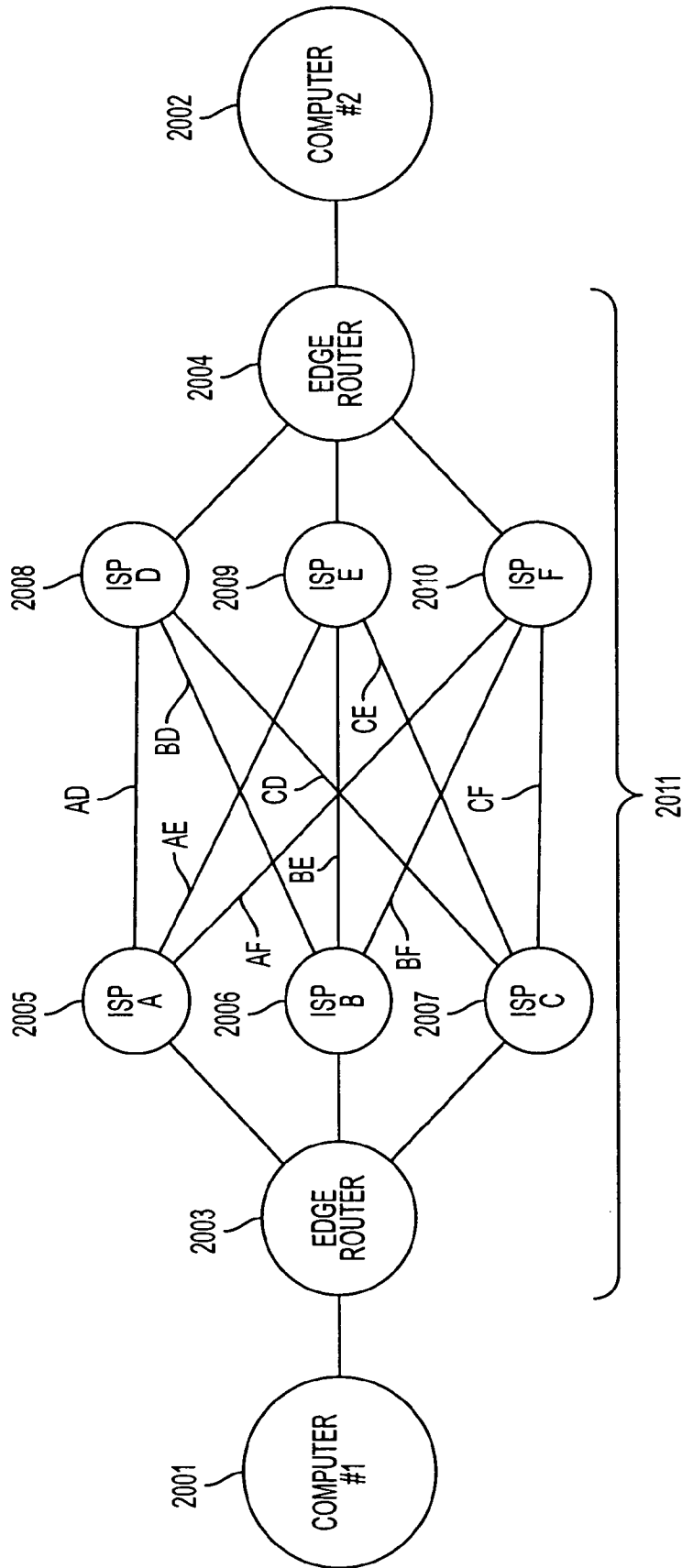


FIG. 20

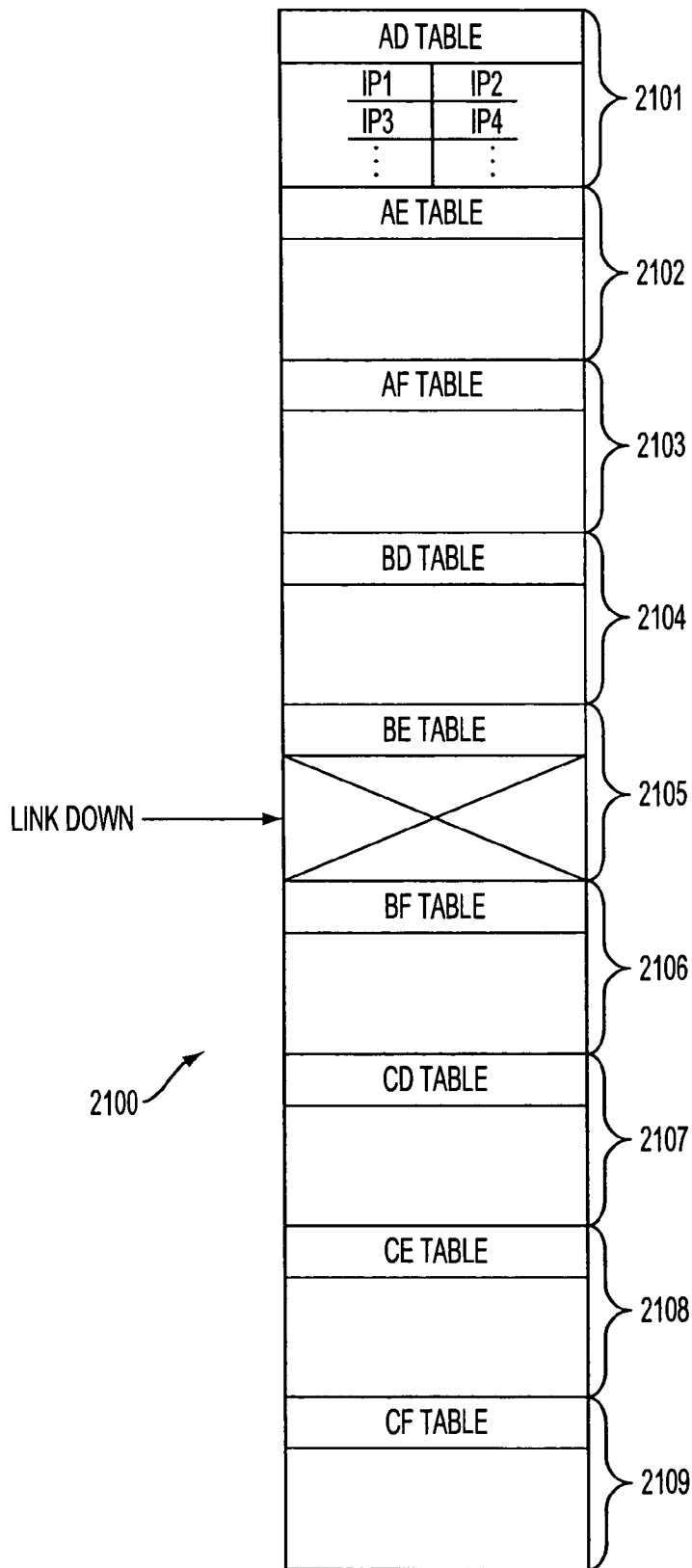


FIG. 21

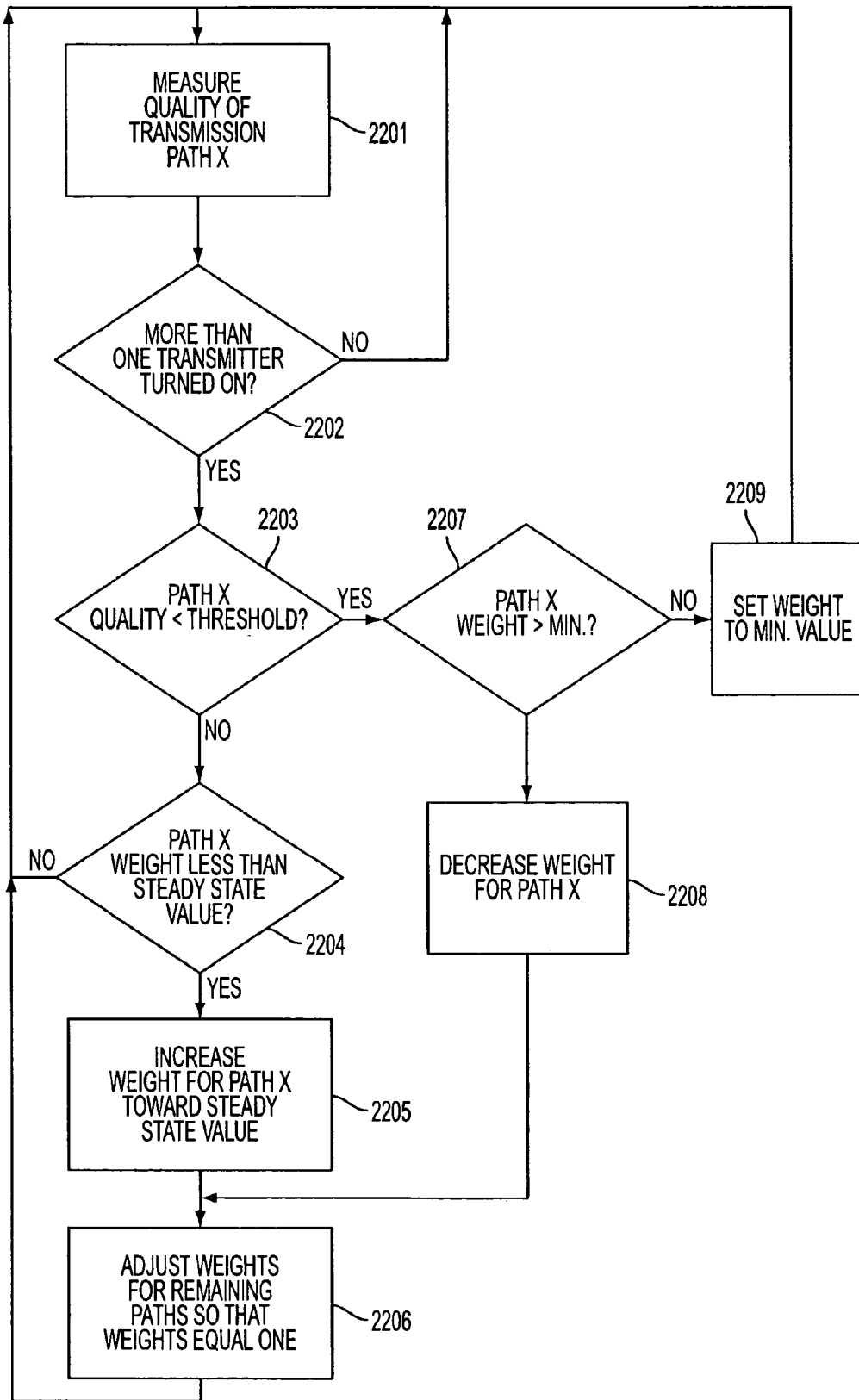


FIG. 22A

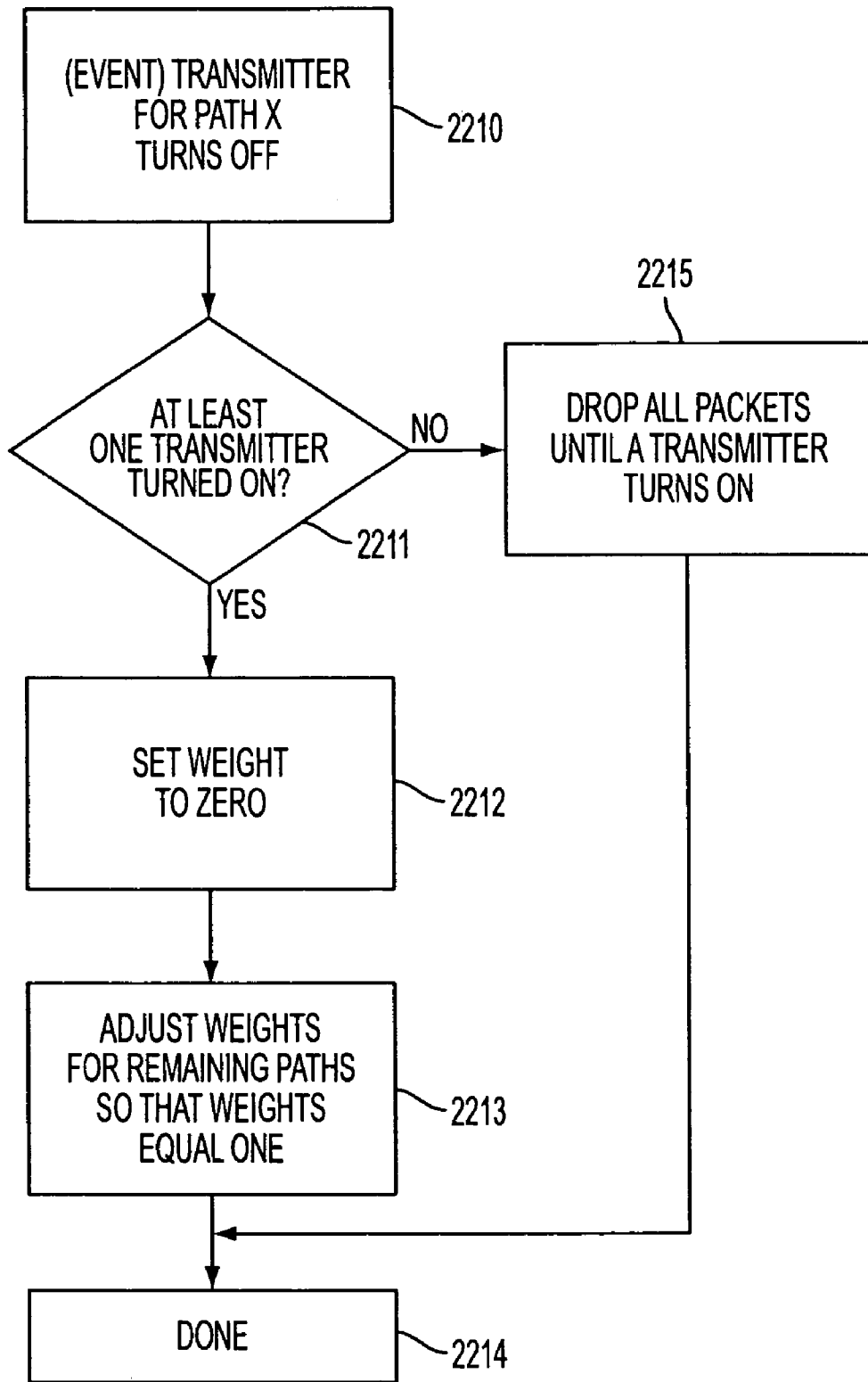


FIG. 22B

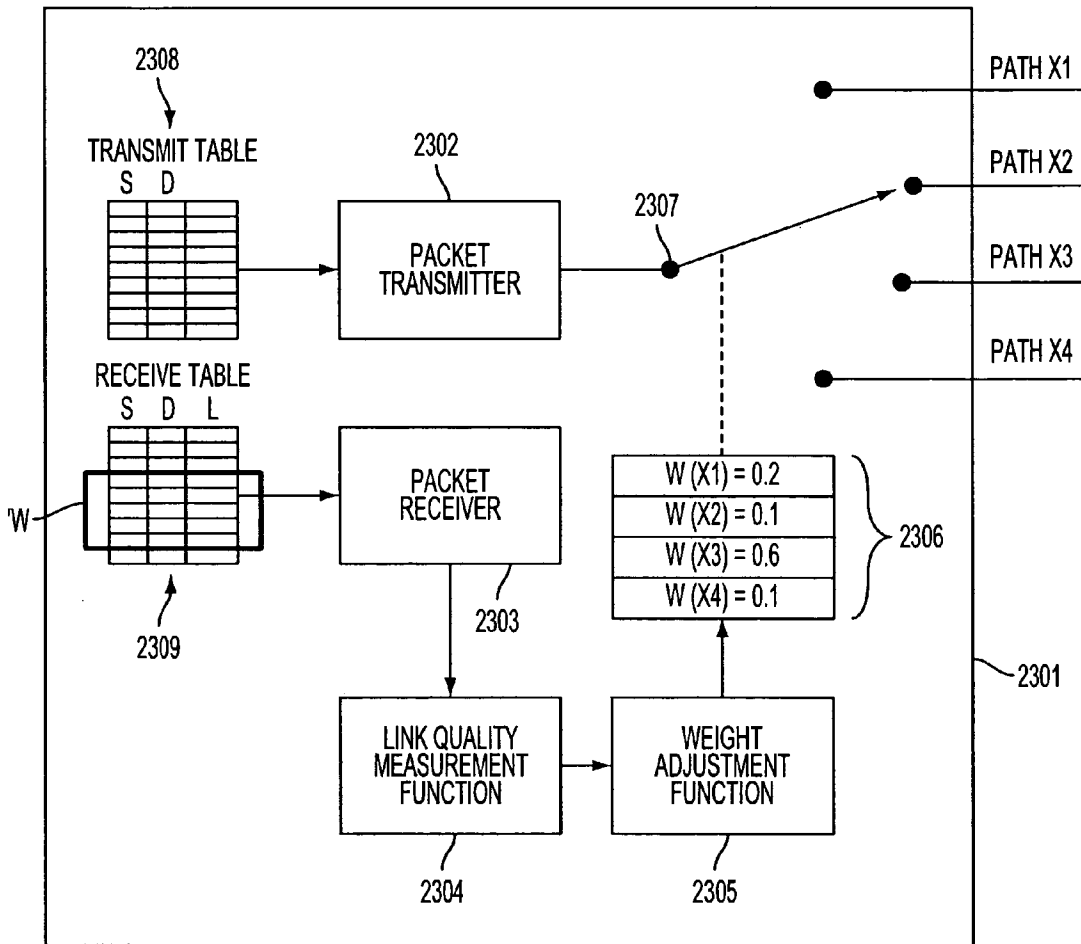


FIG. 23

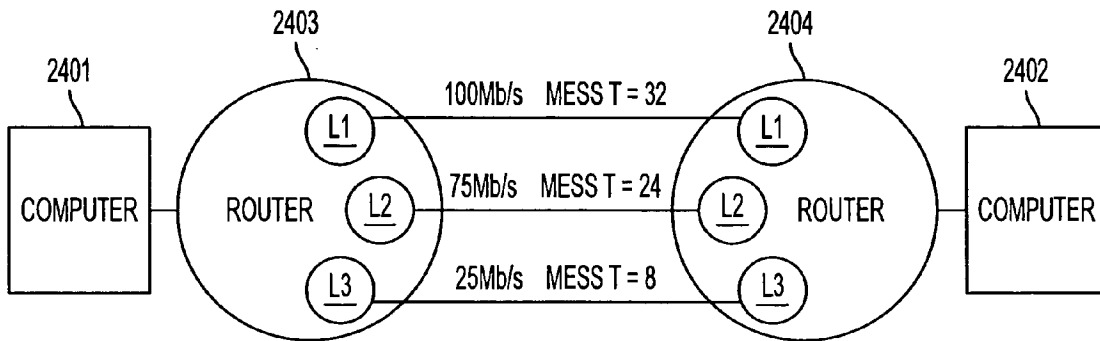


FIG. 24

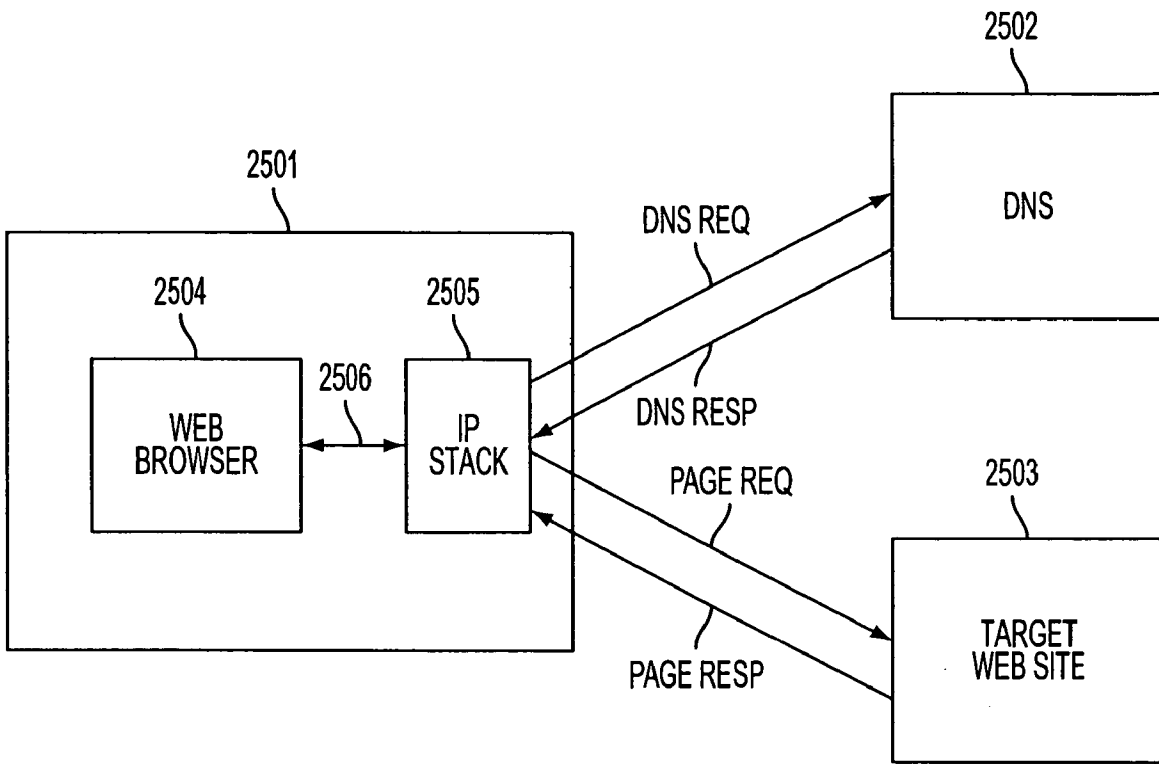


FIG. 25
(PRIOR ART)

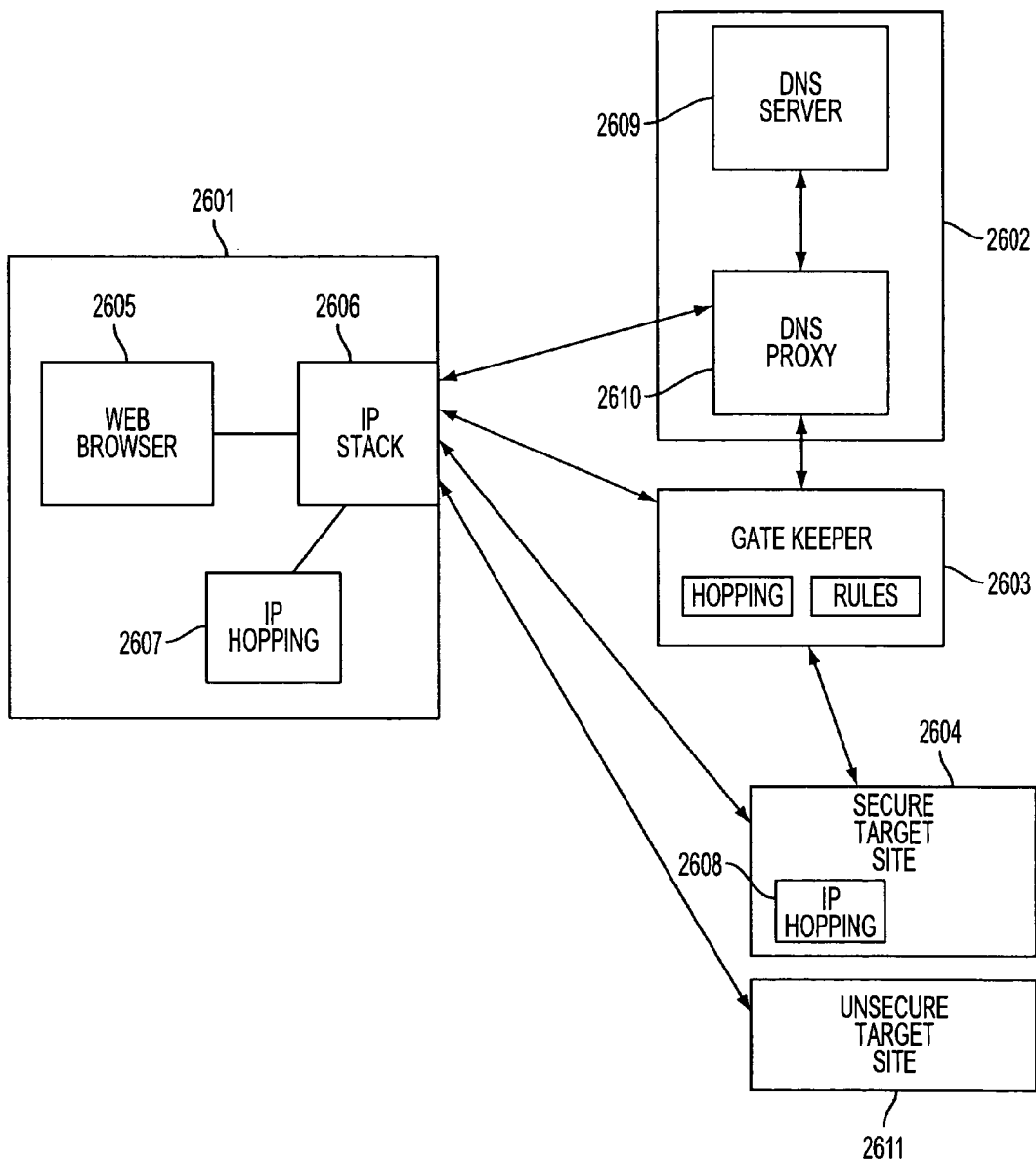


FIG. 26

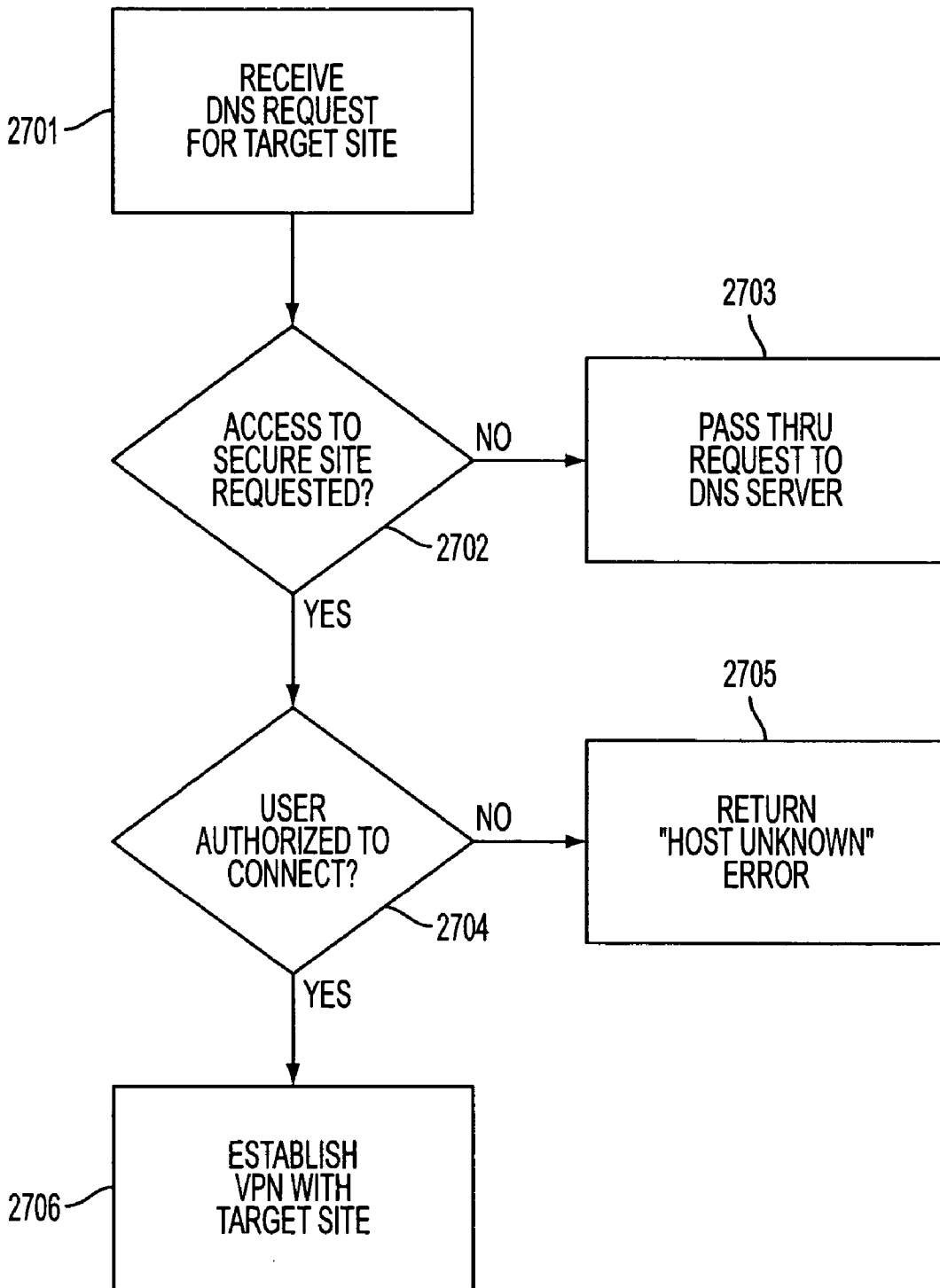


FIG. 27

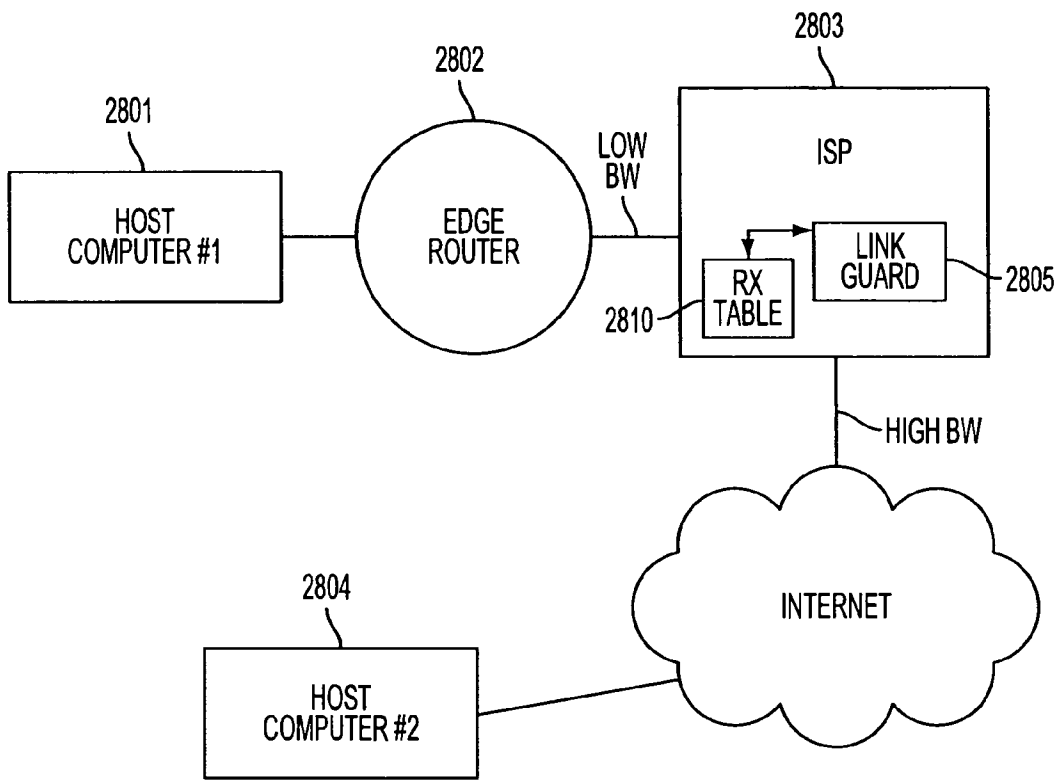


FIG. 28

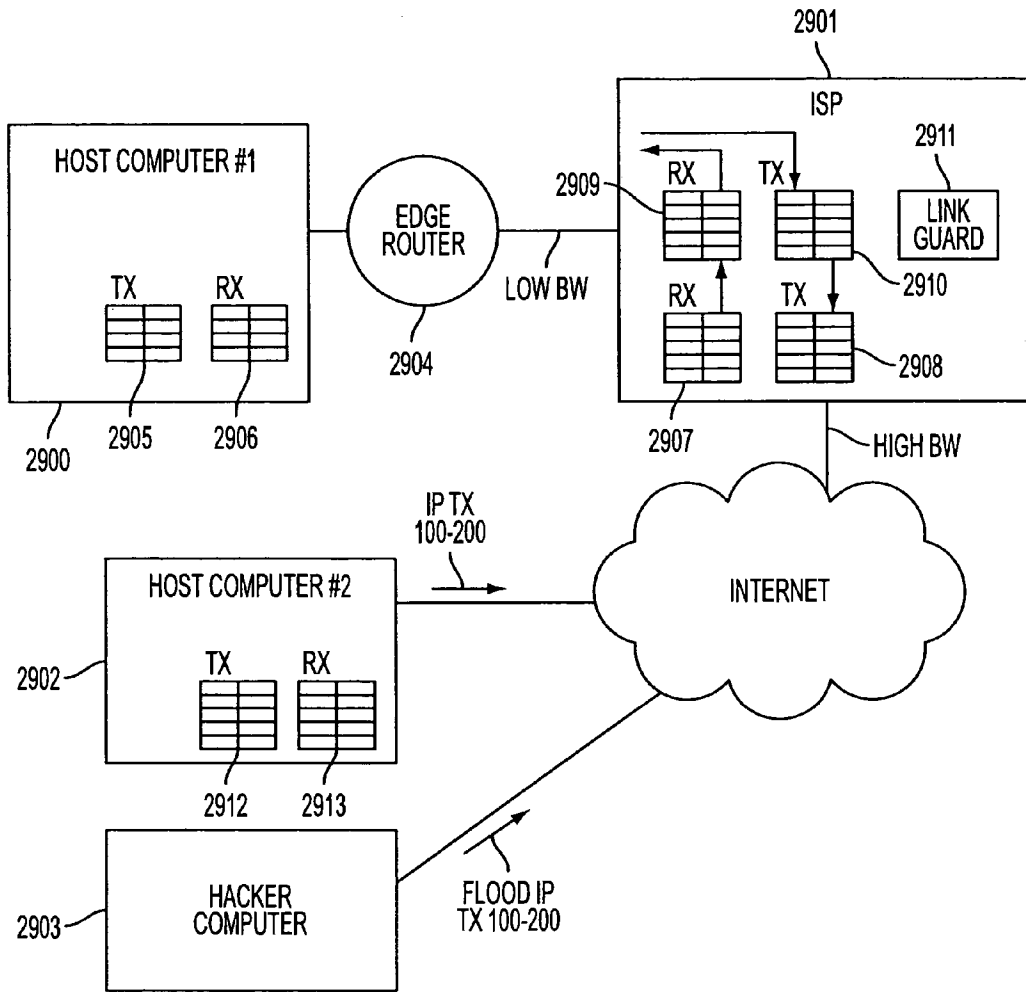


FIG. 29

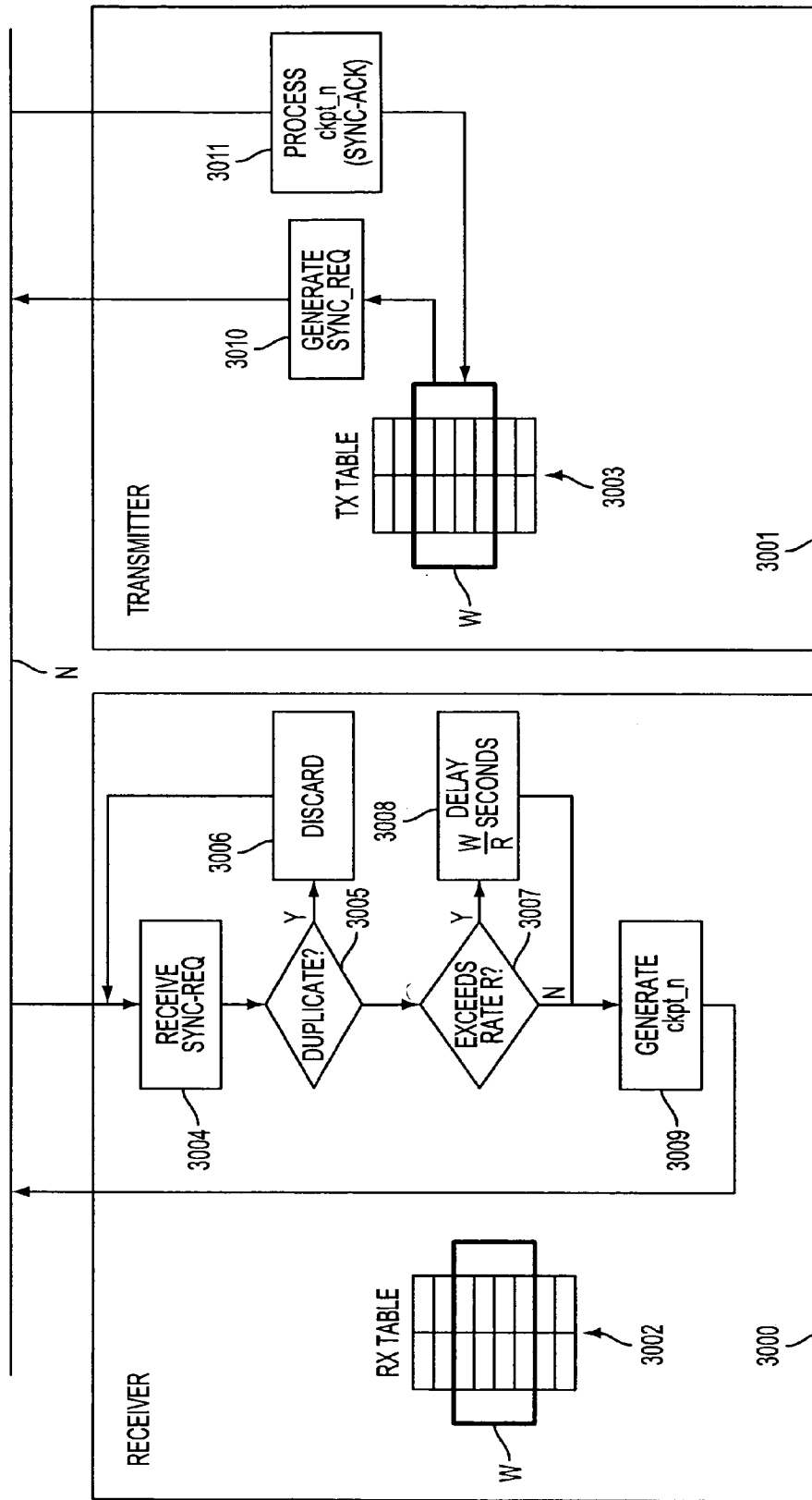


FIG. 30

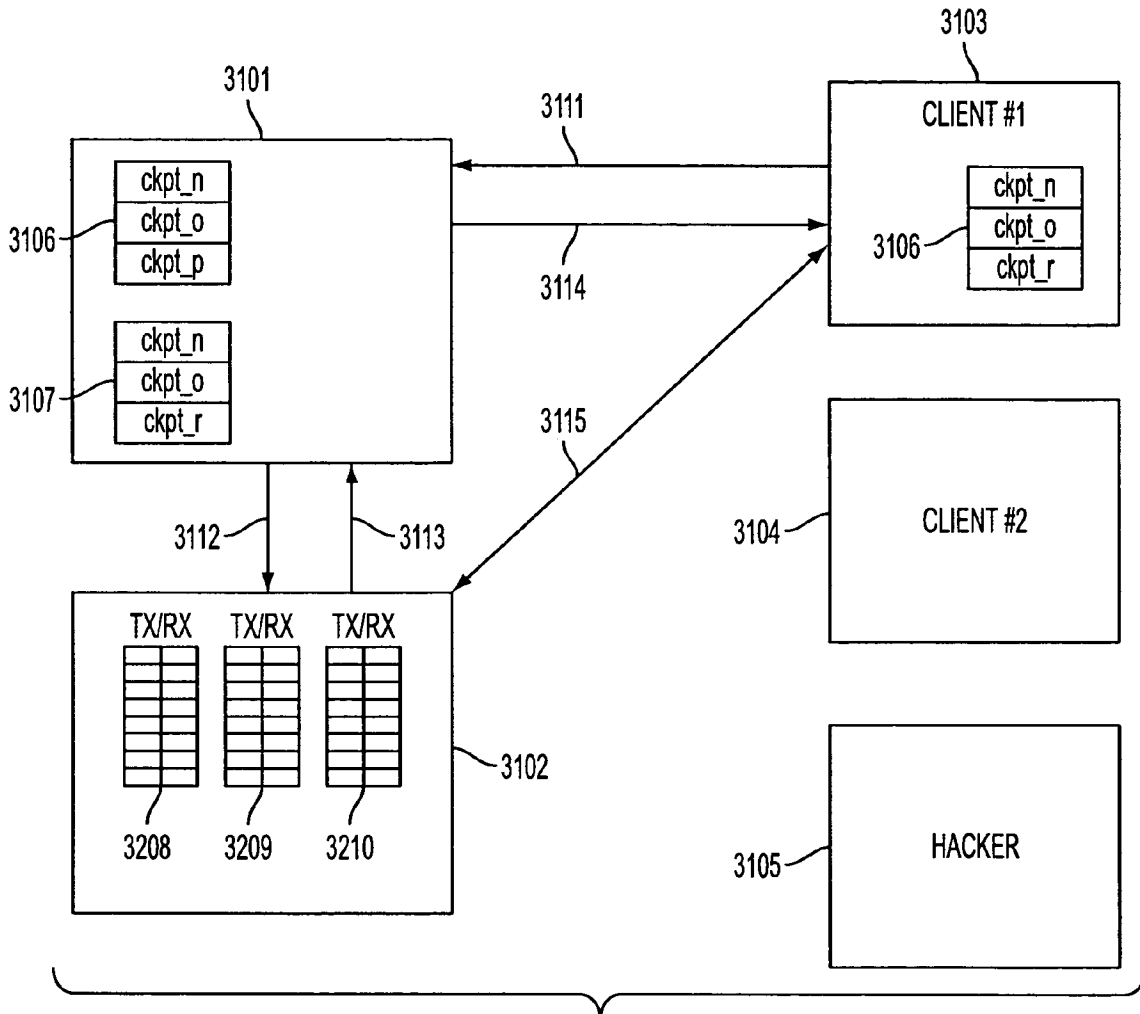


FIG. 31

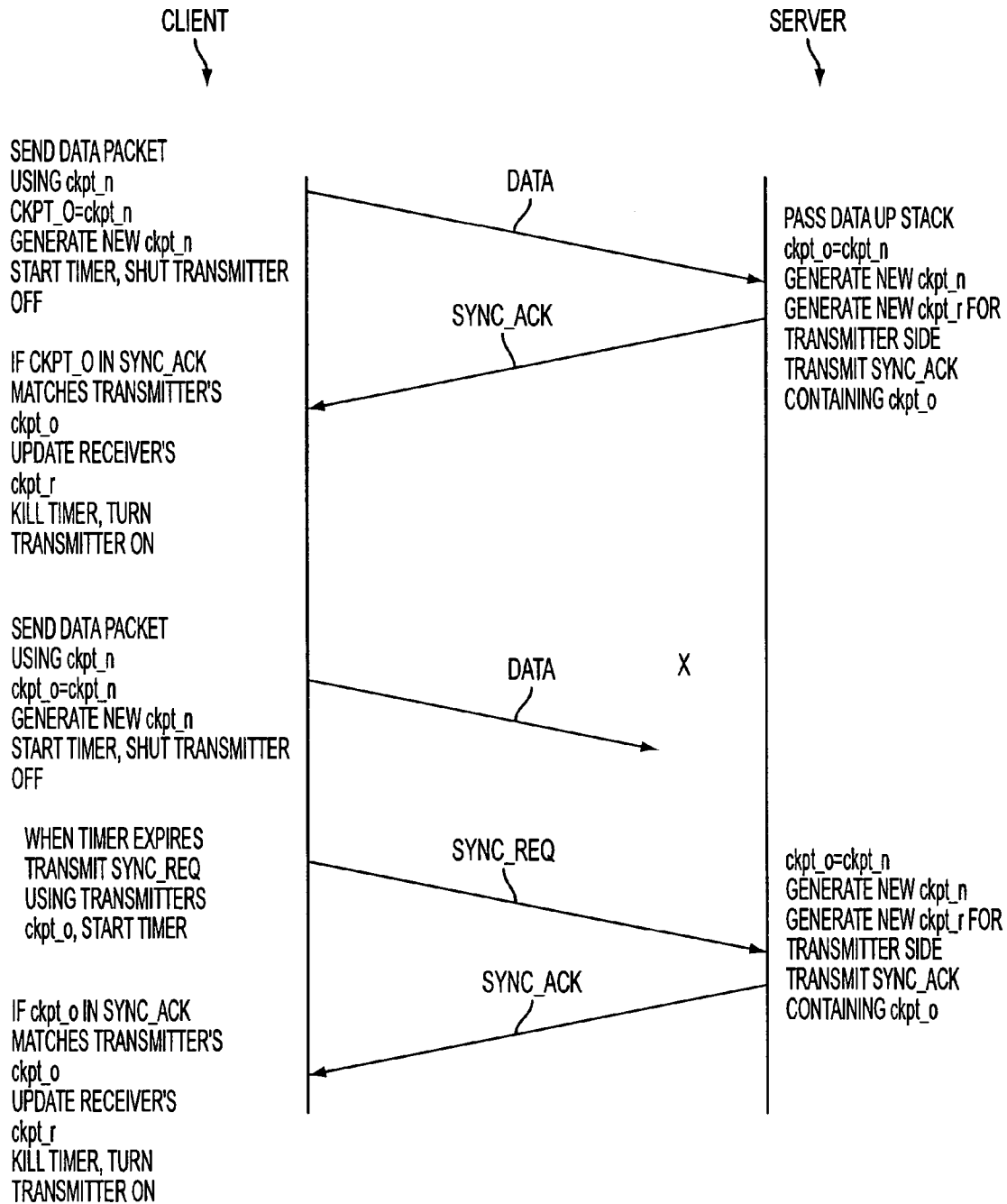


FIG. 32

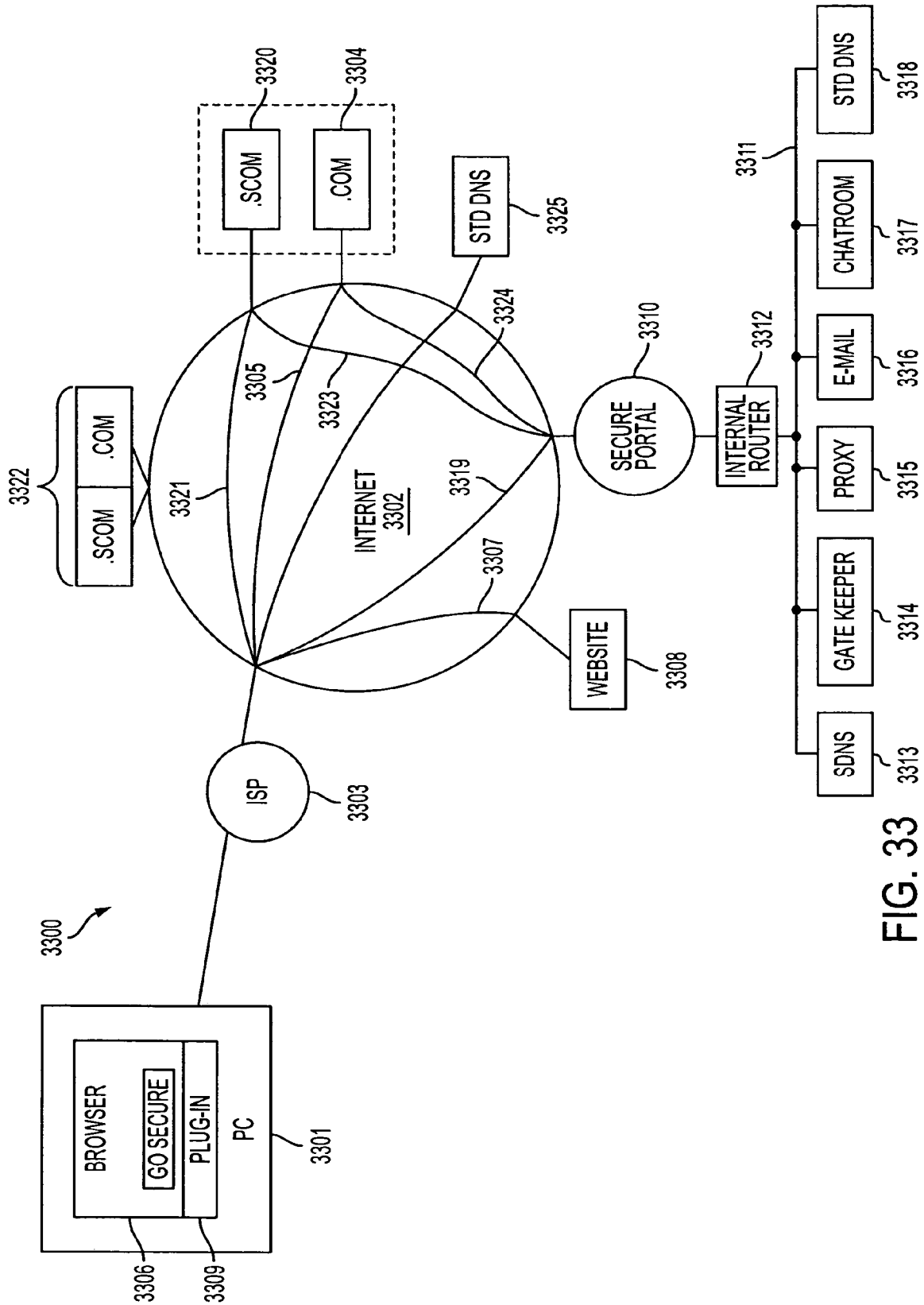


FIG. 33

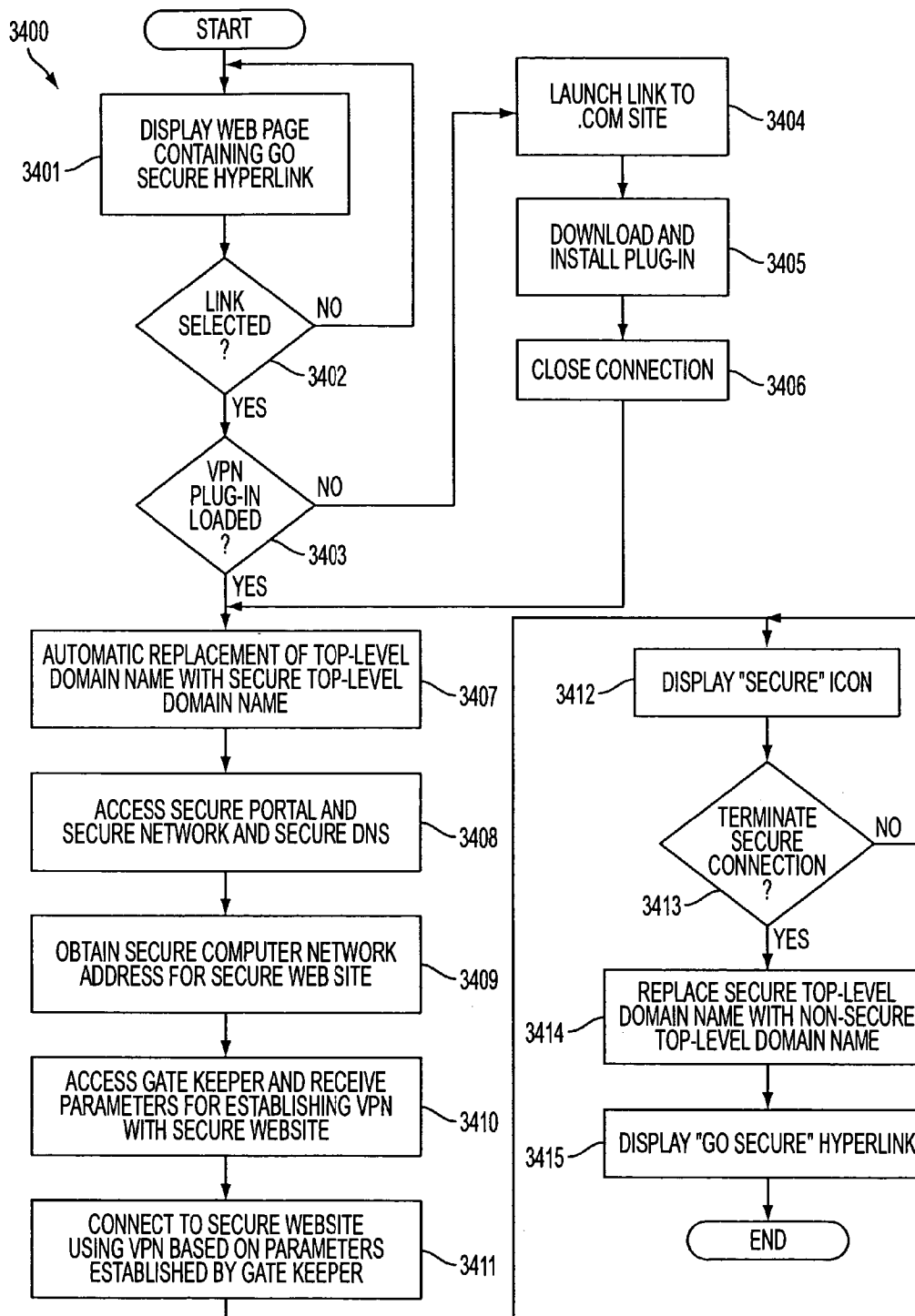


FIG. 34

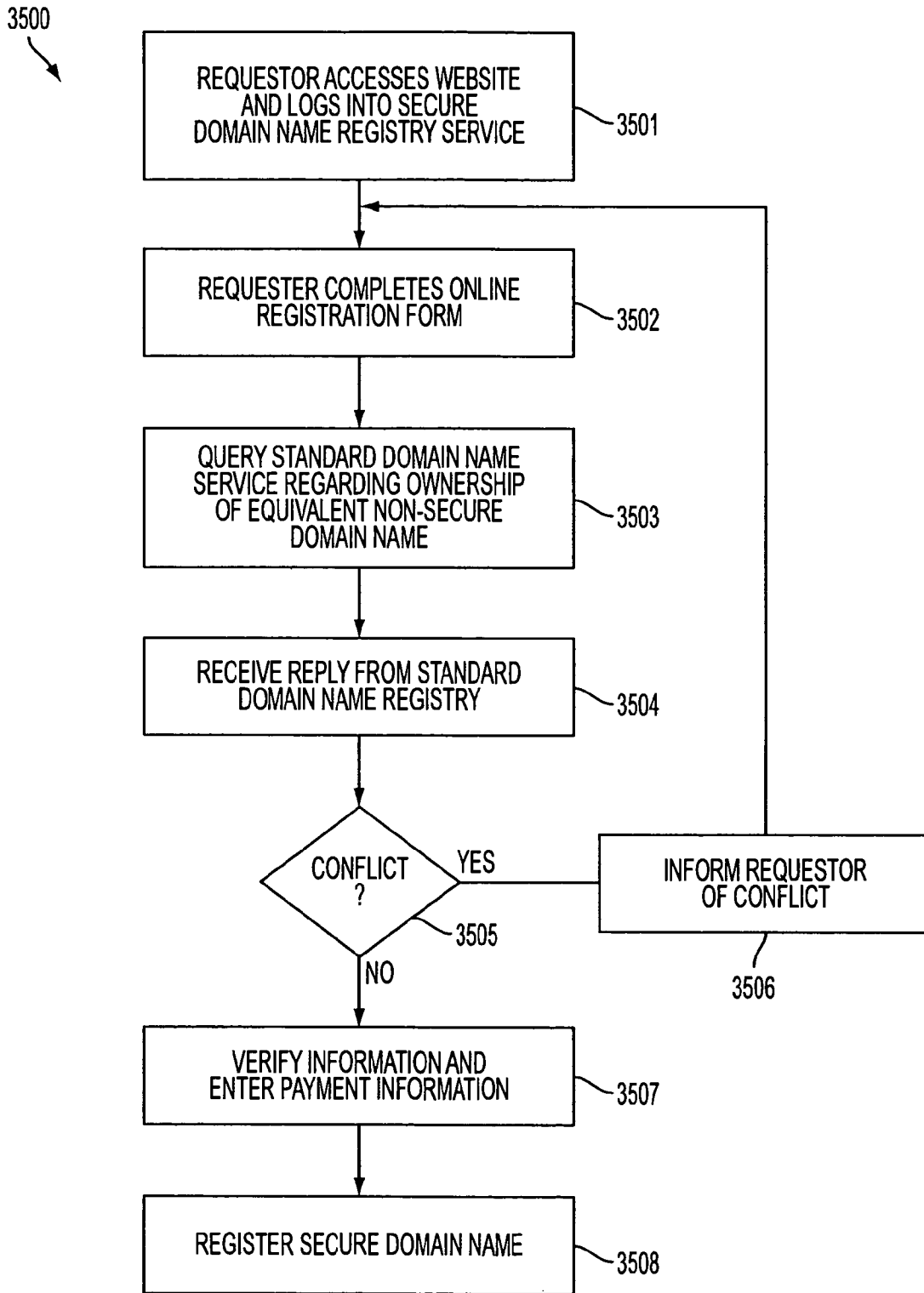


FIG. 35

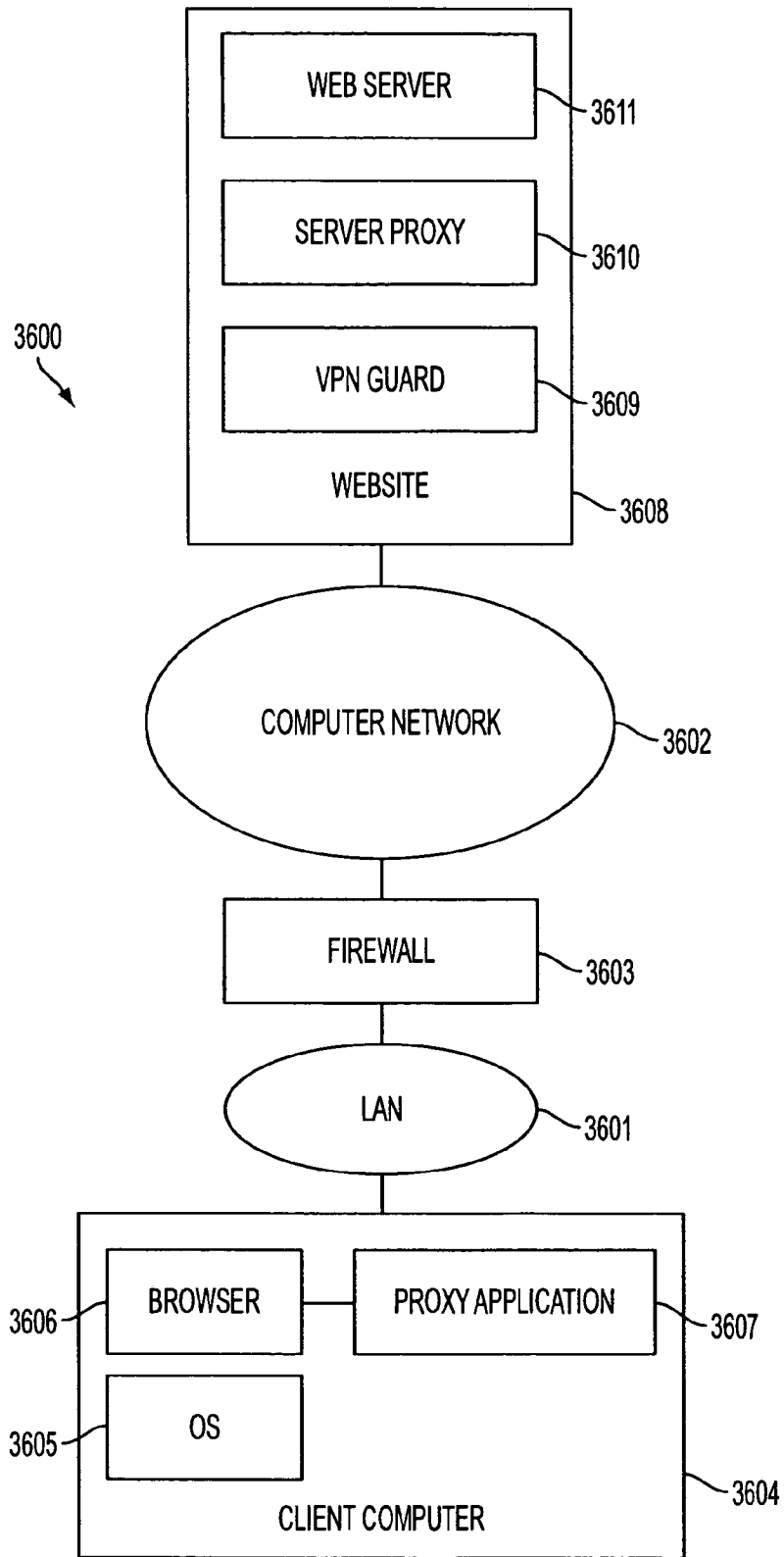


FIG. 36

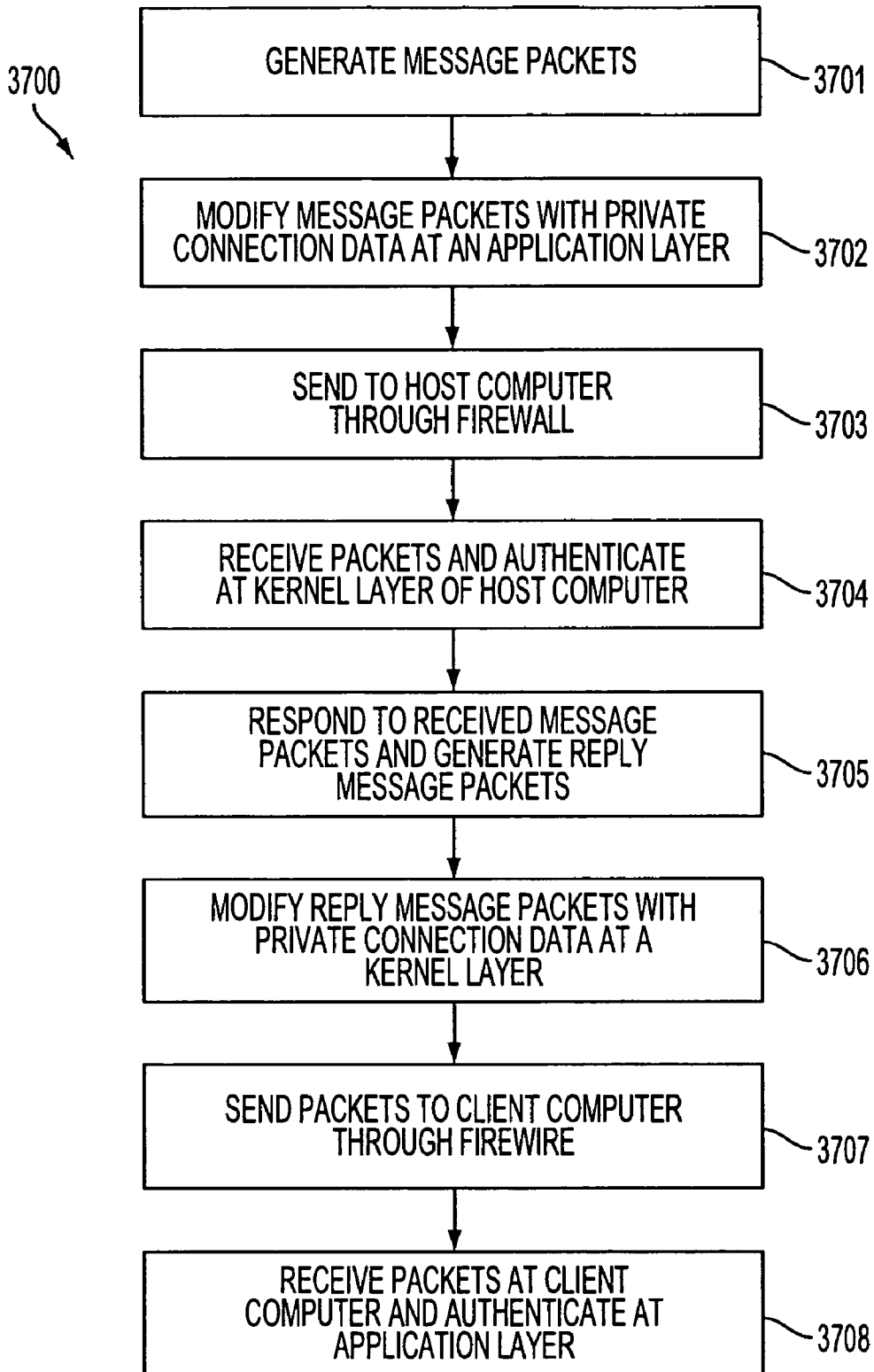


FIG. 37

1

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

CROSS-REFERENCE TO RELATED
APPLICATIONS

This application claims priority from and is a divisional patent application of U.S. application Ser. No. 09/558,209, filed Apr. 26, 2000, now abandoned which is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/504,783, filed on Feb. 15, 2000, now U.S. Pat. No. 6,502,135, issued Dec. 31, 2002, which claims priority from and is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/429,643, filed on Oct. 29, 1999, now U.S. Pat. No. 7,010,604, issued Mar. 7, 2006, The subject matter of U.S. application Ser. No. 09/429,643, which is bodily incorporated herein, derives from provisional U.S. application Nos. 60/106,261 (filed Oct. 30, 1998) and 60/137,704 (filed Jun. 7, 1999). The present application is also related to U.S. application Ser. No. 09/558,210, filed Apr. 26, 2000, and which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

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

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

To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of

2

the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

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

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

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

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

SUMMARY OF THE INVENTION

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

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

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

The IP address of a TARP router can be changed, a feature called IP agility. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or

terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

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

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

To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms “network layer,” “data link layer,” “application layer,” etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IPT are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender’s TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

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

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

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

5

of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

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

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

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

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

In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted

6

between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

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

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

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

7

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

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

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

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

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

8

client computer that has been modified at the kernel layer to containing virtual private connection information in the payload portion of the reply information packet. Preferably, the information packet from the client computer and the reply information packet from the server side are each a UDP protocol information packet. Alternative, both information packets could be a TCP/IP protocol information packet, or an ICMP protocol information packet.

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FIG. 15 shows further details of the checkpoint scheme of FIG. 14.

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

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

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

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

FIG. 20 shows a system employing distributed transmission paths.

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

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

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

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

FIG. 24 shows an example using the system of FIG. 23.

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

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

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

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

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

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

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

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

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

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

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

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

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

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. 2, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers 122–127 that are similar to regular IP routers 128–132 in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets 140. TARP packets 140 are identical to normal IP packet messages that are routed by regular IP routers 128–132 because each TARP packet 140 contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's 140 IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal 110. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet 140 since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal 110.

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

Once the outer layer of decryption is completed by a TARP router 122–127, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet 140 to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet 140 to another TARP router 122–127 or to the destination TARP terminal 110. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to the destination TARP terminal 110. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to a TARP router 122–127 that the current TARP terminal chooses at random. As a result, each TARP packet 140 is routed through some minimum number of hops of TARP routers 122–127 which are chosen at random.

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

A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IP_C. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the

11

TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers **122–127** intervening between the originating **100** and destination **110** TARP terminals. The session key is used to decrypt the payloads of the TARP packets **140** permitting an entire message to be reconstructed.

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

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

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

1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence.
2. An interleave sequence number—an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.
3. A time-to-live (TTL) datum—indicates the number of TARP-router-hops to be executed before the packet

12

reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.

4. Data type identifier—indicates whether the payload contains, for example, TCP or UDP data.
5. Sender's address—indicates the sender's address in the TARP network.
6. Destination address—indicates the destination terminal's address in the TARP network.
7. Decoy/Real—an indicator of whether the packet contains real message data or dummy decoy data or a combination.

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

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

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

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

13

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

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

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

Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of “attacks.” The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing. As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) data-

14

grams as an example; this message will contain the machine’s TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

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

As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

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

15

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

- S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
- S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.
- S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S4. If the packet is a decoy packet, the perishable decoy counter is incremented.
- S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.
- S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.
- S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.
- S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.
- S10. The TARP packet is encrypted using the memorized link key.
- S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

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

- S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.
- S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window. The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.
- S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.
- S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.

16

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

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

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

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

S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.

S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

S44. If the packet is a decoy packet, the perishable decoy counter is incremented.

S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.

S46. The TARP packets are cached until all packets forming an interleave window are received.

S47. Once all packets of an interleave window are received, the packets are deinterleaved.

S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.

S49. The decrypted block is then divided using the window sequence data and the IP_T headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.

S50. The packets are then handed up to the IP layer processes.

1. Scalability Enhancements

The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is

also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

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

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

Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

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

When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling 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.

FIG. 8 shows how a client computer **801** and a TARP router **811** can establish a secure session. When client **801** seeks to establish an IHOP session with TARP router **811**, the client **801** sends "secure synchronization" request ("SSYN") packet **821** to the TARP router **811**. This SSYN packet **821** contains the client's **801** authentication token, and may be sent to the router **811** in an encrypted format. The source and destination IP numbers on the packet **821** are the client's **801** current fixed IP address, and a "known" fixed IP address for the router **811**. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's **801** SSYN packet **821**, the router **811** responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") **822** to the client **801**. This SSYN ACK **822** will contain the transmit and receive hopblocks that the client **801** will use when communicating with the TARP router **811**. The client **801** will acknowledge the TARP router's **811** response packet **822** by generating an encrypted SSYN ACK ACK packet **823** which will be sent from the client's **801** fixed IP address and to the TARP router's **811** known fixed IP address. The client **801** will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet **824**, will be sent with the first {sender, receiver} IP pair in the client's transmit table **921** (FIG. 9), as specified in the transmit hopblock provided by the TARP router **811** in the SSYN ACK packet **822**. The TARP router **811** will respond to the SSI packet **824** with an SSI ACK packet **825**, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table **923**. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client **801** and the TARP router **811** will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client **801** and TARP router **802** may re-establish the secure session by the procedure outlined in FIG. 8 and described above.

While the secure session is active, both the client **901** and TARP router **911** (FIG. 9) will maintain their respective transmit tables **921**, **923** and receive tables **922**, **924**, as provided by the TARP router during session synchronization **822**. It is important that the sequence of IP pairs in the client's transmit table **921** be identical to those in the TARP router's receive table **924**; similarly, the sequence of IP pairs in the client's receive table **922** must be identical to those in the router's transmit table **923**. This is required for the session synchronization to be maintained. The client **901** need maintain only one transmit table **921** and one receive

table 922 during the course of the secure session. Each sequential packet sent by the client 901 will employ the next {send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router 911 will expect each packet arriving from the client 901 to bear the next IP address pair shown in its receive table.

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

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

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

The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given

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

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

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

2. Further Extensions

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

Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or “MAC” addresses in broadcast type network; (2) a self-synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as “frames.” As shown in FIG. 11, for example, a first Ethernet frame 1150 comprises a frame header 1101 and two embedded IP packets IP1 and IP2, while a second Ethernet frame 1160 comprises a different frame header 1104 and a single IP packet IP3. Each frame header gener-

ally includes a source hardware address **1101A** and a destination hardware address **1101B**; other well-known fields in frame headers are omitted from FIG. **11** for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

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

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

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

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

track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as “secure” packets or “secure communications” to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

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

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

Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process every incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine’s MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as “promiscuous” mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack otherwise it is discarded.

One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine’s CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to

use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical-layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

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

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

Reference will now be made to FIGS. 12A and 12B in order to describe the many combinations and features that follow the inventive principles. As explained above, two computer nodes 1201 and 1202 are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (1204 and 1217, respectively) contains a modified element 1205 and 1216 that performs certain functions that deviate from the standard communication protocols. In particular, computer node 1201 implements a first “hop” algorithm 1208X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node 1201 maintains a transmit table 1208 containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node 1202. As each new IP packet is formed, the next sequential entry out of the sender’s transmit table 1208 is used to populate the IP source, IP destination, and IP header extension field (e.g.,

discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

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

Node 1202 maintains a similar transmit table 1221 for creating IP packets and frames destined for node 1201 using a potentially different hopping algorithm 1221X, and node 1201 maintains a matching receive table 1209 using the same algorithm 1209X. As node 1202 transmits packets to node 1201 using seemingly random IP source, IP destination, and/or discriminator fields, node 1201 matches the incoming packet values to those falling within window W1 maintained in its receive table. In effect, transmit table 1208 of node 1201 is synchronized (i.e., entries are selected in the same order) to receive table 1222 of receiving node 1202. Similarly, transmit table 1221 of node 1202 is synchronized to receive table 1209 of node 1201. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. 12A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be “hopped” rather than all three as illustrated.

In accordance with another aspect of the invention, hardware or “MAC” addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node 1201 further maintains a transmit table 1210 using a transmit algorithm 1210X to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields 1101A and 1101B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202. Similarly, node 1202 maintains a different transmit table 1223 containing source and destination hardware addresses that is synchronized with a corresponding receive table 1211 at node 1201. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

FIG. 12B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as “promiscuous” mode, a

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

In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks. (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

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

B. Extending the Address Space

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

Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients

communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

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

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

A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that 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.

In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

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

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

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

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

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

decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

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

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

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

The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large-integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

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

A “checkpoint” scheme can be used to regain synchronization between a sender and a receiver that have fallen out

of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

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

1. In the transmitter, ckpt_o (“checkpoint old”) is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o (“checkpoint old”) is the IP pair that receives repeated SYNC_REQ packets from the transmitter.
2. In the transmitter, ckpt_n (“checkpoint new”) is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n (“checkpoint new”) is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver’s window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.
3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14).

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

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

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

If an interloper intercepts the “sync request” messages and tries to interfere with communication by sending new

ones, it will be ignored if the synchronization has been established or it will actually help to re-establish synchronization.

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

E. Random Number Generator with a Jump-Ahead Capability

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

Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead n steps efficiently. An LCR generates random numbers X₁, X₂, X₃ . . . X_k starting with seed X₀ using a recurrence

$$X_i = (a X_{i-1} + b) \text{ mod } c \tag{1}$$

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

$$X_i = ((a^i(X_0 + b) - b) / (a - 1)) \text{ mod } c \tag{2}$$

enables the jump-ahead capability. The factor aⁱ 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:

$$X_i = (a^i(X_0(a-1) + b) - b) / (a-1) \text{ mod } c. \tag{3}$$

It can be shown that:

$$(a^i(X_0(a-1) + b) - b) / (a-1) \text{ mod } c = ((a^i \text{ mod } ((a-1)c) (X_0(a-1) + b) - b) / (a-1)) \text{ mod } c \tag{4}$$

(X₀(a-1)+b) can be stored as (X₀(a-1)+b) mod c, b as b mod c and compute aⁱ mod ((a-1)c) (this requires O(log(i)) steps).

A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every n packets. The window would commence n IP pairs from the start of the previous window. Using X_j^w, the random number at the jth checkpoint, as X₀ and n as i, a node can store aⁿ mod ((a-1)c) once per LCR and set

$$X_{j+1}^w = X_{n/(j+1)} = ((a^n \text{ mod } ((a-1)c) (X_j^w(a-1) + b) - b) / (a-1)) \text{ mod } c \tag{5}$$

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

Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme.

An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack—against the encryptor.

F. Random Number Generator Example

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

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

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

((91(X_i30+4)-4)/30)mod 15 (7)

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

TABLE 1

Table with 6 columns: I, X_i, (X_i30 + 4), 91 (X_i30 + 4) - 4, ((91 (X_i30 + 4) - 4)/30), X_{i+3}. Rows show calculations for i=1, 4, 7, 10, 13.

G. Fast Packet Filter

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

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

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

- 2. There are 2^24 (~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).
- 3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B-trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n-1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the 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."

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

There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. 16). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

A presence vector will have a 1 in the 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.

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

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

I. Further Synchronization Enhancements

A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO (“Out of Order”) and $2 \times \text{WINDOW_SIZE} + \text{OoO}$ 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.

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.

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

Another embodiment incorporating various inventive principles is shown in FIG. 20. In this embodiment, a message transmission system includes a first computer 2001 in communication with a second computer 2002 through a network 2011 of intermediary computers. In one variant of this embodiment, the network includes two edge routers 2003 and 2004 each of which is linked to a plurality of Internet Service Providers (ISPs) 2005 through 2010. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. 20, which is a representative configuration only and is not intended to be limiting. Each connection between ISPs is labeled in FIG. 20 to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element 2005) to ISP D (element 2008)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

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

3. Continuation-in-Part Improvements

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

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

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

When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the synchronization function (i.e., no packets are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

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

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

Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over

time for a path, one specific implementation uses the “windowing” concepts described above to evaluate transmission path health.

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

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

Beginning in step 2201, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

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

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

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

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

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

Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as

37

desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

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

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

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

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

Link quality measurement function 2304 can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function 2304. According to one embodiment,

38

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.

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

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

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

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

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 $0 < \beta \leq 1$ that determines the damping rate of P.

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

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

Suppose that a first link L1 can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L2 can sustain 75 Mb/s and has a window size of 24; and link L3 can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200 Mb/s. The steady state traffic weights are 0.5 for link L1; 0.375 for link L2, and 0.125 for link L3. MIN=1 Mb/s, THRESH=0.8 MESS_T for each link, $\alpha=0.75$ and $\beta=0.5$. These traffic weights will remain stable until a link stops for synchronization or reports

a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link L1 receives a SYNC_ACK containing a MESS_R of 24, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 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 0.005, link L2's traffic weight value would be decreased to 0.74625, and link L3's traffic weight value would be decreased to 0.24875.

4. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.2525, while link L2's traffic weight value would be decreased to 0.560625 and link L3's traffic weight value would be decreased to 0.186875.

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

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

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

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

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

This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack 2505) to a DNS 2502 to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application 2504, which is then able to use the IP address to communicate with the host 2503 through separate transactions such as PAGE REQ and PAGE RESP.

In the conventional architecture shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the

name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

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

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

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

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

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

Had the user requested lookup of a non-secure web site such as site 2611, DNS proxy would merely pass through to

41

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

Gatekeeper **2603** can be implemented on a separate computer (as shown in FIG. **26**) or as a function within modified DNS server **2602**. In general, it is anticipated that gatekeeper **2703** facilitates the allocation and exchange of information needed to communicate securely, such as using “hopped” IP addresses. Secure hosts such as site **2604** are assumed to be equipped with a secure communication function such as an IP hopping function **2608**.

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

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

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

If the user is not authorized to access the secure site, then a “host unknown” message is returned (step **2705**). If the user has sufficient security privileges, then in step **2706** a secure VPN is established between the user’s computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user’s computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of this application, any of various fields can be “hopped” (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

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

Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client’s DNS request would be received

42

by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

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

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

Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client’s DNS request and forward it to gatekeeper **2603**. Gatekeeper **2603** would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server **2610** to return an error message to the client.

C. Large Link to Small Link Bandwidth Management

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

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

Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer **2801** across high bandwidth link HIGH BW. Normally, host computer **2801** would be able to quickly reject the packets since they would not fall within the acceptance window

permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer **2801**. Consequently, the link to host computer **2801** is effectively flooded before the packets can be discarded.

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

In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc **401**], the packets have IP protocols **420** and **421**. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP’s link guard, **2805**, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid. According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP **2903** maintains a copy **2910** of the receive table used by host computer **2901**. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard **2805** validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc **2104**].

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

As shown in FIG. **29**, for example, suppose that a first host computer **2900** is communicating with a second host computer **2902** over the Internet, and the path includes a high bandwidth link HIGH BW to an ISP **2901** and a low bandwidth link LOW BW through an edge router **2904**. In accordance with the basic architecture described above, first host computer **2900** and second host computer **2902** would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables **2905**, **2906**, **2912** and **2913**. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

Suppose that a nefarious computer hacker **2903** was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP **2901**, and that these packets are being forwarded over a low-bandwidth link. Hacker com-

puter **2903** could thus “flood” packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer **3000** would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard **2911** would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of-service flood attack could, however, still disrupt non-VPN traffic.

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

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

D. Traffic Limiter

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

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

Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets. A compliant transmitter would not issue new SYNC_REQ

45

messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate, each receiver could defer issuing a new CKPT_N until $M \times N \times W/R$ 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.

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

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

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

To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of $M \times N \times W/R$ seconds after the last SYNC_REQ has been received and accepted, $2 \times M \times N \times W/R$ seconds after next to the last SYNC_REQ has been received and accepted, $C \times M \times N \times W/R$ seconds after $(C-1)^{th}$ to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

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

46

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

In accordance with the improvements described above, receiving computer 3000 performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. 30.

In step 3004, receiving computer 3000 receives the SYNC_REQ message. In step 3005, a check is made to determine whether the request is a duplicate. If so, it is discarded in step 3006. In step 3007, a check is made to determine whether the SYNC_REQ received from transmitter 3001 was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step 3008 the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

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

E. Signaling Synchronizer

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

One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets. When a packet is received from a

known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

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

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

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

Thereafter, client 3103 communicates with transport server 3102 using the normal hopping techniques described above. It will be appreciated that although signaling server 3101 and transport server 3102 are illustrated as being two separate computers, they could of course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. 31 differently from as shown without departing from the inventive principles.

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

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

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

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

The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

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

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

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

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

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

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

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

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

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

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

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

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

The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication

method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and operates on computer 3301 in a well-known manner.

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

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

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

If, at step 3403, the object determines that the software module has been installed, flow continues to step 3407. If, at step 3403, the object determines that the software module has not been installed, flow continues to step 3404 where a non-VPN communication link 3307 is launched between computer 3301 and a website 3308 over computer network 3302 in a well-known manner. Website 3308 is accessible by all computer terminals connected to computer network 3302 through a non-VPN communication link. Once connected to website 3308, a software module for establishing a secure communication link over computer network 3302 can be downloaded and installed. Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over com-

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

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

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

Because the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown. According to the invention, software module 3409 contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module 3309 accesses a secure portal 3310 that interfaces a secure network 3311 to computer network 3302. Secure network 3311 includes an internal router 3312, a secure domain name service (SDNS) 3313, a VPN gatekeeper 3314 and a secure proxy 3315. The secure network can include other network services, such as e-mail 3316, a plurality of chatrooms (of which only one chatroom 3317 is shown), and a standard domain name service (STD DNS) 3318. Of course, secure network 3311 can include other resources and services that are not shown in FIG. 33.

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

query from software module 3309 based on the particular information hopping technique used for VPN communication link 3319.

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

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

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

At step 3411, software module 3309 accesses secure server 3320 through VPN communication link 3321 based on the VPN resources allocated by VPN gatekeeper 3314. At step 3412, web browser 3306 displays a secure icon indicating that the current communication link to server 3320 is a secure VPN communication link. Further communication between computers 3301 and 3320 occurs via the VPN, e.g., using a “hopping” regime as discussed above. When VPN link 3321 is terminated at step 3413, flow continues to step 3414 where software module 3309 automatically replaces the secure top-level domain name with the corresponding non-secure top-level domain name for server 3304. Browser 3306 accesses a standard DNS 3325 for obtaining the

53

non-secure URL for server **3304**. Browser **3306** then connects to server **3304** in a well-known manner. At step **3415**, browser **3306** displays the “go secure” hyperlink or icon for selecting a VPN communication link between terminal **3301** and server **3304**. By again displaying the “go secure” hyperlink, a user is informed that the current communication link is a non-secure, non-VPN communication link.

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

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

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

At step **3503**, the secure domain name registry service at website **3308** queries a non-secure domain name server database, such as standard DNS **3322**, using, for example, a whois query, for determining ownership information relating to the non-secure domain name corresponding to the requested secure domain name. At step **3504**, the secure domain name registry service at website **3308** receives a reply from standard DNS **3322** and at step **3505** determines whether there is conflicting ownership information for the corresponding non-secure domain name. If there is no conflicting ownership information, flow continues to step **3507**, otherwise flow continues to step **3506** where the requestor is informed of the conflicting ownership information. Flow returns to step **3502**.

When there is no conflicting ownership information at step **3505**, the secure domain name registry service (website **3308**) informs the requestor that there is no conflicting ownership information and prompts the 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**.

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

54

situation and prompts the requestor for acquiring the corresponding equivalent non-secure domain name for an increased fee. By accepting the offer, the present invention automatically registers the corresponding equivalent non-secure domain name with standard DNS **3325** in a well-known manner. Flow then continues to step **3508**.

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

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

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

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

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

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

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

A client computer **3604** is connected to LAN **3601** in a well-known manner. Client computer **3604** includes an operating system **3605** and a web browser **3606**. Operating system **3605** provides kernel mode functions for operating client computer **3604**. Browser **3606** is an application program for accessing computer network resources connected to LAN **3601** and computer network **3602** in a well-known manner. According to the present invention, a proxy application **3607** is also stored on client computer **3604** and

operates at an application layer in conjunction with browser **3606**. Proxy application **3607** operates at the application layer within client computer **3604** and when enabled, modifies unprotected, unencrypted message packets generated by browser **3606** by inserting data into the message packets that are used for forming a virtual private connection between client computer **3604** and a server computer connected to LAN **3601** or computer network **3602**. According to the invention, a virtual private connection does not provide the same level of security to the client computer as a virtual private network. A virtual private connection can be conveniently authenticated so that, for example, a denial of service attack can be rapidly rejected, thereby providing different levels of service that can be subscribed to by a user.

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

Referring to FIG. 37, at step **3701**, unprotected and unencrypted message packets are generated by browser **3606**. At step **3702**, proxy application **3607** modifies the payload portion of all message packets by tunneling the data for forming a virtual private connection between client computer **3604** and a destination server computer into the payload portion. At step, **3703**, the modified message packets are sent from client computer **3604** to, for example, website (server computer) **3608** over computer network **3602**.

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

Server proxy portion **3610** also operates at the kernel layer within website **3608** and catches incoming message

packets from client computer **3604** at the VPN level. At step **3705**, server proxy portion **3610** authenticates the message packets at the kernel level within host computer **3604** using the destination IP address, UDP ports and discriminator fields. The authenticated message packets are then forwarded to the authenticated message packets to web server portion **3611** as normal TCP web transactions.

At step **3705**, web server portion **3611** responds to message packets received from client computer **3604** in accordance with the particular nature of the message packets by generating reply message packets. For example, when a client computer requests a webpage, web server portion **3611** generates message packets corresponding to the requested webpage. At step **3706**, the reply message packets pass through server proxy portion **3610**, which inserts data into the payload portion of the message packets that are used for forming the virtual private connection between host computer **3608** and client computer **3604** over computer network **3602**. Preferably, the data for forming the virtual private connection is contains field-hopping data, such as described above in connection with VPNs. Server proxy portion **3610** operates at the kernel layer within host computer **3608** to insert the virtual private connection data into the payload portion of the reply message packets. Preferably, the modified message packets sent by host computer **3608** to client computer **3604** conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol.

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

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

What is claimed is:

1. A method for accessing a secure computer network address, comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.
2. The method according to claim 1, wherein the step of receiving the secure domain name includes steps of:
 - receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

57

automatically generating a secure domain name corresponding to the non-secure domain name.

3. The method according to claim 2, wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display. 5

4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.

5. The method according to claim 4, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence. 10

6. The method according to claim 4, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network. 15

7. The method according to claim 4, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer. 20

8. The method according to claim 4, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values. 25

9. The method according to claim 4, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields. 30

10. The method according to claim 1, wherein the virtual private network includes the Internet.

11. The method according to claim 1, wherein the secure domain name has a top-level domain name that includes one of .com, .net, .org, .edu, .mil or .gov. 35

12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.

13. The method of claim 1, 40
 wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;
 wherein sending the query message comprises sending the query message at the client computer; 45
 wherein receiving the response message comprises receiving the response message at the client computer, wherein sending the access request message comprises sending the access request message at the client computer. 50

14. The method of claim 1, performed by a software module.

15. The method of claim 1, performed by a client computer.

16. The method of claim 2, wherein receiving the command comprises receiving the command at a client computer from a user. 55

17. A computer-readable storage medium, comprising:
 a storage area; and
 computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:
 receiving a secure domain name;
 sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name; 65

58

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

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

18. The computer-readable medium according to claim 17, wherein the step of receiving the secure domain name includes steps of:

receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

automatically generating a secure domain name corresponding to the non-secure domain name.

19. The computer-readable medium according to claim 18, wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display. 20

20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.

21. The computer-readable medium according to claim 20, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

22. The computer-readable medium according to claim 20, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network. 25

23. The computer-readable medium according to claim 20, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer. 30

24. The computer-readable medium according to claim 20, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values. 35

25. The computer-readable medium according to claim 20, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields. 40

26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.

27. The computer-readable medium according to claim 17, wherein the secure domain name has a top-level domain name that includes one of .com, .net, .org, .edu, .mil or .gov. 45

28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.

29. The computer-readable medium according to claim 17, 50
 wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;
 wherein sending the query message comprises sending the query message at the client computer; 55

59

wherein receiving the response message comprises receiving the response message at the client computer, wherein sending the access request message comprises sending the access request message at the client computer.

30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.

31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.

32. The computer-readable medium according to claim 18, wherein receiving the command comprises receiving the command at a client computer from a user.

33. A data processing apparatus, comprising:
a processor, and

memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:
receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
sending an access request message to the secure computer network address using a virtual private network communication link.

34. The apparatus of claim 33, wherein the step of receiving the secure domain name includes steps of:

receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

60

automatically generating a secure domain name corresponding to the non-secure domain name.

35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.

36. The apparatus of claim 35, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

37. The apparatus of claim 35, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

38. The apparatus of claim 35, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

39. The apparatus of claim 35, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

40. The apparatus of claim 35, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

41. The apparatus of claim 33, wherein the secure domain name has a top-level domain name that includes one of .com, .net, .org, .edu, .mil or .gov.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,188,180 B2
APPLICATION NO. : 10/702486
DATED : March 6, 2007
INVENTOR(S) : Victor Larson et al.

Page 1 of 1


It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

IN PATENT TITLE PAGE:

Item (75), Inventors, delete "Durham" and insert therefor -- Dunham --.

Signed and Sealed this

Seventh Day of August, 2007

A handwritten signature in black ink on a light gray dotted background. The signature reads "Jon W. Dudas" in a cursive style.

JON W. DUDAS

Director of the United States Patent and Trademark Office

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2009-11-25
	First Named Inventor	LARSON, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		3755-121

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

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

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

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² 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				
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		
Filing Date		2009-11-25
First Named Inventor	LARSON, et al.	
Art Unit		
Examiner Name		
Attorney Docket Number	3755-121	

1	Exhibit 2 "Aventail Connect v3.1/v2.6 Administrator's Guide", pgs. 1-120, 1996-1999.	<input type="checkbox"/>
2	Exhibit 3, "Windows NT Server, Virtual Private Network: An Overview", pgs. 1-28, 1998.	<input type="checkbox"/>
3	Exhibit 4, "Network Working Group Request For Comments 1035", pgs. 1-56, 1987.	<input type="checkbox"/>
4	Exhibit 5, "Kusiur" Building and Managing Virtual Private Networks, pgs 1-396, 1998.	<input type="checkbox"/>
5	Exhibit 6, "Kaufman et al.," Implementing IPsec, pgs. 1-280, 1999.	<input type="checkbox"/>
6	Exhibit 7, "James Galvin" Public Key Distribution Secure DNS, pgs. 1-12, 1996.	<input type="checkbox"/>
7	Exhibit 8A, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs 1-137, 1998-1999.	<input type="checkbox"/>
8	Exhibit 8B, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs. 138-275, 1998-1999.	<input type="checkbox"/>
9	Exhibit 9, "Windows NT Technical Support: Hands On, Self Paced Training for Supporting Version 4.0", pgs. 1-106, 1998.	<input type="checkbox"/>
10	Exhibit 10, "Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, pgs. 1-30, 1997.	<input type="checkbox"/>
11	Exhibit 11, "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources, pgs. 1-216, 2000.	<input type="checkbox"/>

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

Application Number		
Filing Date		2009-11-25
First Named Inventor	LARSON, et al.	
Art Unit		
Examiner Name		
Attorney Docket Number	3755-121	

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

EXAMINER SIGNATURE

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

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

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

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

Application Number			
Filing Date		2009-11-25	
First Named Inventor	LARSON, et al.		
Art Unit			
Examiner Name			
Attorney Docket Number		3755-121	

CERTIFICATION STATEMENT

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

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

OR

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

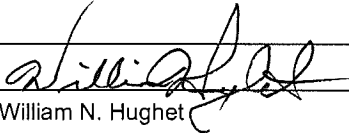
See attached certification statement.

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

None

SIGNATURE

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

Signature		Date (YYYY-MM-DD)	2009-11-25
Name/Print	William N. Hughet	Registration Number	44481

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

Privacy Act Statement

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

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

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

Appendix A

Citations to Exemplary Description in the Aventail Connect v3.1/v2.6 Administrator's Guide Reference*

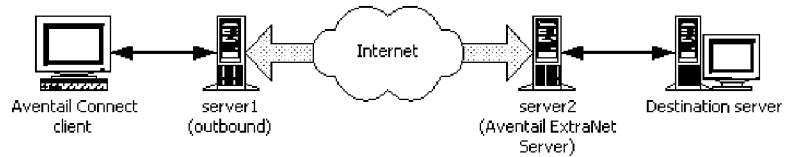
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. The first response to these concerns has been the development of security firewalls—software barriers that control the flow of information. But firewalls are not designed to handle complex security issues, such as monitoring network usage, providing private communication over public networks, and enabling remote users to gain secure access to internal network resources.</p> <p>Page 12: b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.</p> <ul style="list-style-type: none"> • It sends the list of authentication methods enabled in the configuration file • Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. • It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1. <p>Page 46: SOCKS v5 servers often require user authentication before allowing access. Aventail Connect authentication modules display dialog boxes that prompt users to enter username and password information as well as other authentication credentials.</p> <p>The current Aventail Connect authentication modules are SOCKS v4 Identification, Username / Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password).</p> <p>Page 62: Once servers and destinations are defined, you can direct SOCKS traffic through successive extranet (SOCKS) servers.</p> <p>Page 66: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. This capability is provided in Aventail Connect 3.1 by the Aventail MultiProxy feature. Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining.</p> <p>Page 72:</p>

* - The cited passages are an indication of where in the Aventail reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

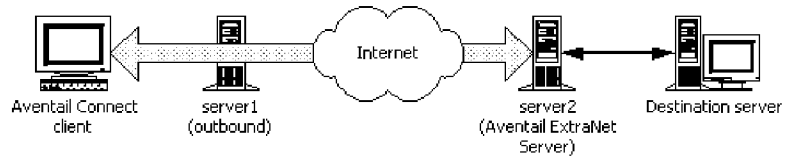
7,188,180 Claim Elements


Description for Claimed Elements in the Aventail Prior Art Reference

PROXY CHAINING: Server1 appears as a user to server2.



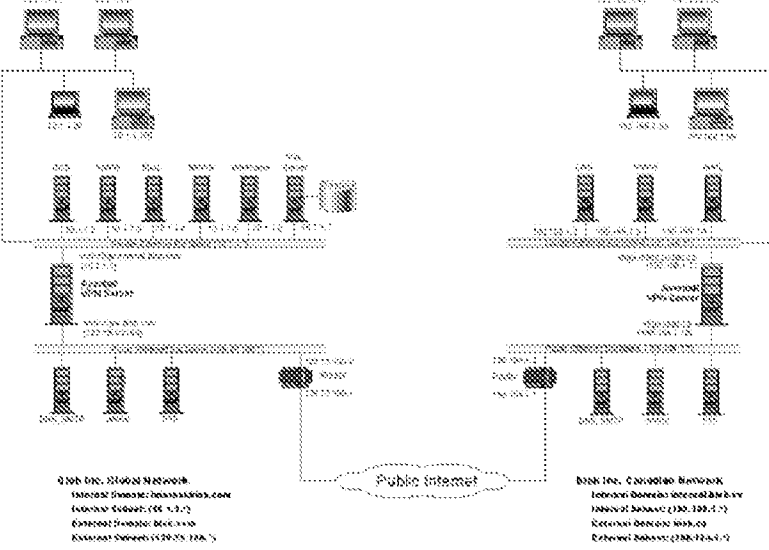
MULTIPROXY: The user authenticates with server2 directly.




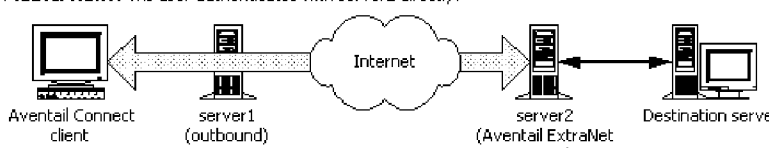

 **Authenticated and encrypted tunnel**
 In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.

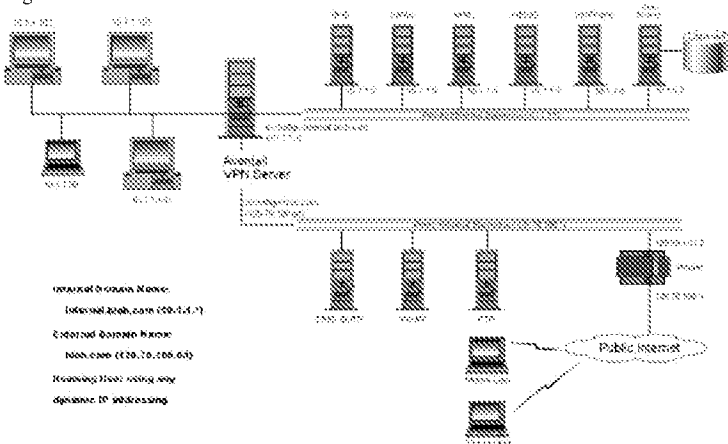
Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.

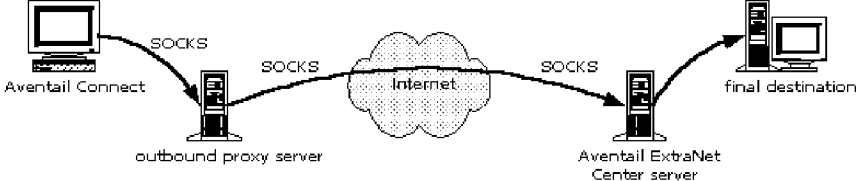
Page 79:

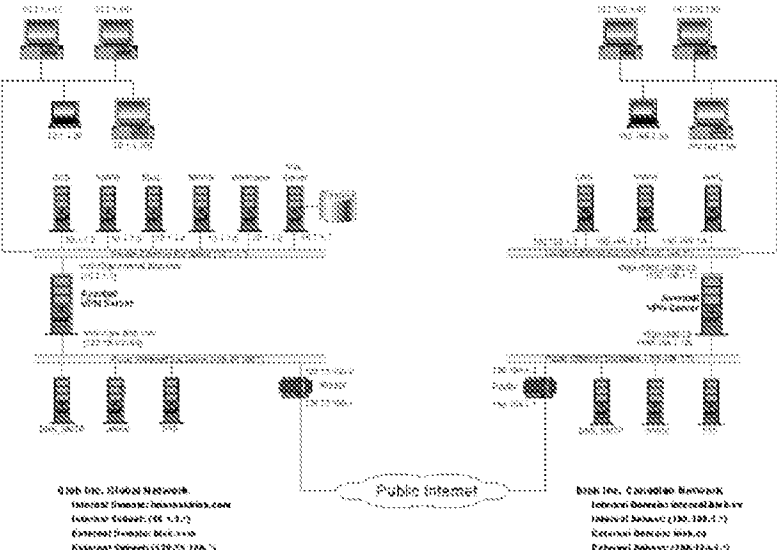
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p>
receiving a secure domain name;	<p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p> <p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <ul style="list-style-type: none"> • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. <p>Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution.</p> <p>Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.</p>
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <ul style="list-style-type: none"> • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet.</p> <p>Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically.</p> <p>Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.</p> <p>Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.</p> <p>Page 69: The client application requests access to the destination server.</p> <p>Page 72:</p> <p>PROXY CHAINING: Server1 appears as a user to server2.</p>  <p>MULTIPROXY: The user authenticates with server2 directly.</p>  <div data-bbox="552 1302 958 1438" style="border: 1px solid black; padding: 5px;">  <p>Authenticated and encrypted tunnel</p> <p>In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.</p> </div> <p>Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the</p>



7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>private LAN for mobile employees and partners.</p> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p> <p>Page 77:</p>  <p>Example Corporate Network Design using Mobile VPN</p> <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p> <p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p>
<p>4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 68: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server.</p>

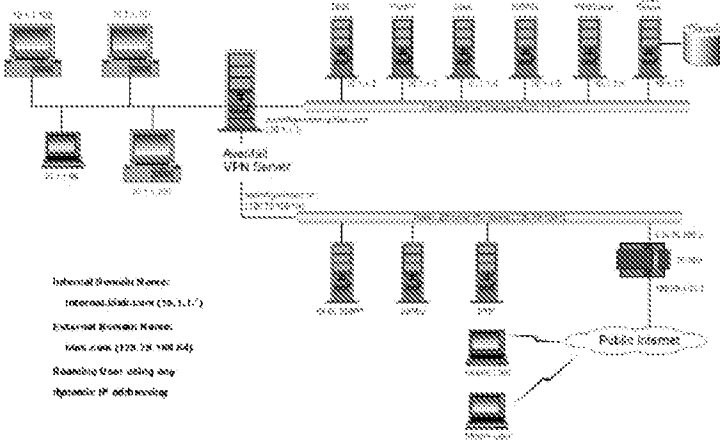
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.</p> <p>Page 69: In the following diagram, the Aventail ExtraNet Server acts as both a destination and a server. It is a destination because a proxy server routes traffic to it. It is a server because it routes traffic to the final destination.</p>  <p>The diagram illustrates a network path. On the left, a computer icon labeled 'Aventail Connect' is connected via a curved arrow labeled 'SOCKS' to a server rack icon labeled 'outbound proxy server'. From the 'outbound proxy server', another curved arrow labeled 'SOCKS' points to a cloud icon labeled 'Internet'. From the 'Internet', a third curved arrow labeled 'SOCKS' points to another server rack icon labeled 'Aventail ExtraNet Center server'. Finally, a fourth curved arrow labeled 'SOCKS' points from the 'Aventail ExtraNet Center server' to a computer icon labeled 'final destination'.</p> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p>
<p>10. The method according to claim 1, wherein the virtual private network includes the Internet.</p>	<p>Page 5: Aventail Corporation is the leading vendor of extranet software. Its extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet.</p> <p>Page 8: Windows TCP/IP networking applications (such as telnet, e-mail, Web browsers, and ftp) use WinSock to gain access to networks or the Internet. WinSock is the core component of TCP/IP under Windows, and is the interface that most Windows applications use to communicate to TCP/IP.</p> <p>Page 79:</p>

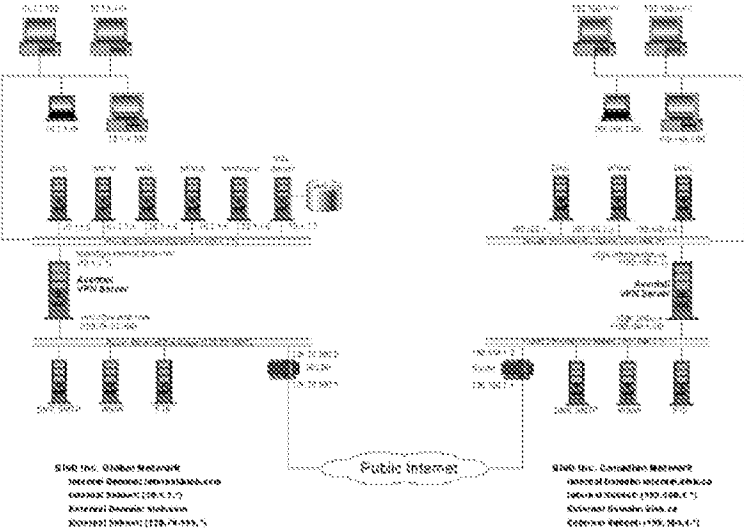
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p>
<p>12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet.</p> <p>Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.</p> <p>Pages 12-13: When the SOCKS negotiation is completed, Aventail Connect notifies the application. Form the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the</p>

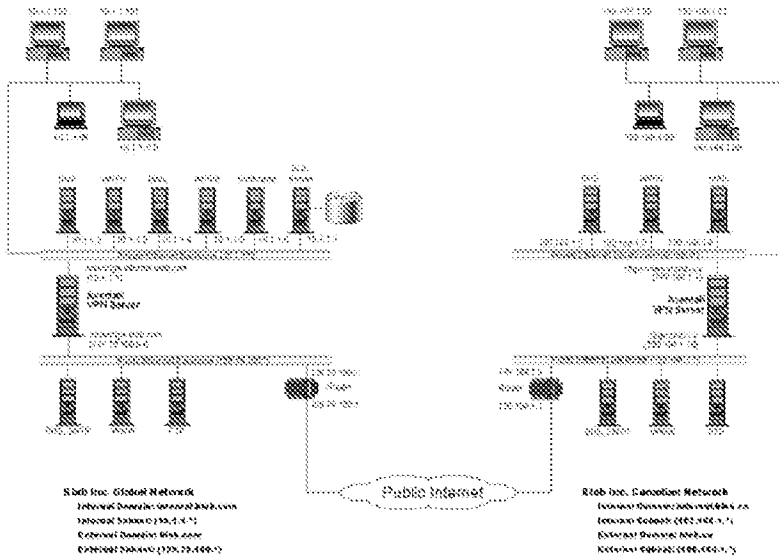
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>TCP handshaking.</p> <p>Page 69: Once the connection between the client and the Aventail ExtraNet Server is established, the output server simply relays the data.</p> <p>Page 69: The client application requests access to the destination server.</p> <p>Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.</p>
13. The method of claim 1,	
<p>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.</p>
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>• If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.</p> <p>Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution.</p> <p>Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.</p>
<p>wherein receiving the response message comprises receiving the response</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
message at the client computer,	<p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>• If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.</p> <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p>
wherein sending the access request message comprises sending the access request message at the client computer.	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet.</p> <p>Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically.</p> <p>Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.</p> <p>Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.</p> <p>Page 69: The client application requests access to the destination server.</p> <p>Page 72:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>PROXY CHAINING: Server1 appears as a user to server2.</p>  <p>MULTIPROXY: The user authenticates with server2 directly.</p>  <div data-bbox="552 1029 966 1165" style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">↔ Authenticated and encrypted tunnel</p> <p>In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.</p> </div> <p>Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.</p> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p> <p>Page 77:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p>Example Corporate Network Design using Mobile VPN</p> <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p> <p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p>
14. The method of claim 1, performed by a software module.	See claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer).
15. The method of claim 1, performed by a client computer.	See claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer). Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the user's desktop.
17. A computer-readable storage medium, comprising:	Page 14: Regardless of platform, Aventail Connect can be delivered on CD or as a network-delivered, self-extracting archive file. Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files.

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location.</p> <p>Page 31: When you load a package, Customizer reads the setup control file to determine what information the package contains. Customizer uses this information to populate the Customizer Editor window. Customizer also reads the configuration file(s) into memory; configuration files are stored in memory to facilitate adding them to and removing them from a package.</p> <p>Page 79:</p>  <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p>
a storage area; and	<p>Page 14: Regardless of platform, Aventail Connect can be delivered on CD or as a network-delivered, self-extracting archive file.</p> <p>Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files.</p> <p>Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves</p>

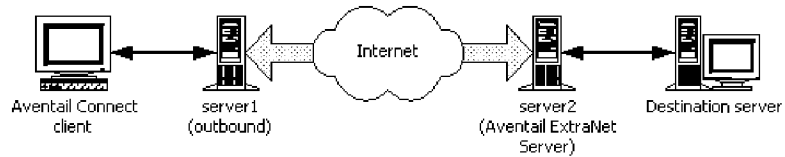
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location.</p> <p>Page 31: When you load a package, Customizer reads the setup control file to determine what information the package contains. Customizer uses this information to populate the Customizer Editor window. Customizer also reads the configuration file(s) into memory; configuration files are stored in memory to facilitate adding them to and removing them from a package.</p> <p>Page 79:</p>  <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p>
<p>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>Page 14: Regardless of platform, Aventail Connect can be delivered on CD or as a network-delivered, self-extracting archive file.</p> <p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. The first response to these concerns has been the development of security firewalls—software barriers that control the flow of information. But firewalls are not designed to handle complex security issues, such as monitoring network usage, providing private communication over public</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>networks, and enabling remote users to gain secure access to internal network resources.</p> <p>Page 12:</p> <p>b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.</p> <ul style="list-style-type: none"> • It sends the list of authentication methods enabled in the configuration file • Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. • It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1. <p>Page 46: SOCKS v5 servers often require user authentication before allowing access. Aventail Connect authentication modules display dialog boxes that prompt users to enter username and password information as well as other authentication credentials.</p> <p>The current Aventail Connect authentication modules are SOCKS v4 Identification, Username / Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password).</p> <p>Page 62: Once servers and destinations are defined, you can direct SOCKS traffic through successive extranet (SOCKS) servers.</p> <p>Page 66: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. This capability is provided in Aventail Connect 3.1 by the Aventail MultiProxy feature. Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining.</p> <p>Page 72:</p>

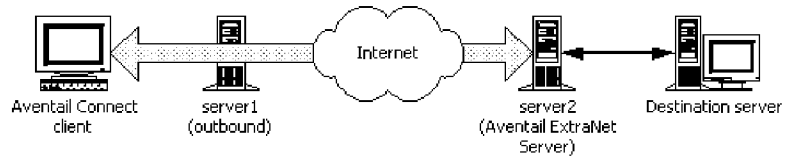
7,188,180 Claim Elements


Description for Claimed Elements in the Aventail Prior Art Reference

PROXY CHAINING: Server1 appears as a user to server2.



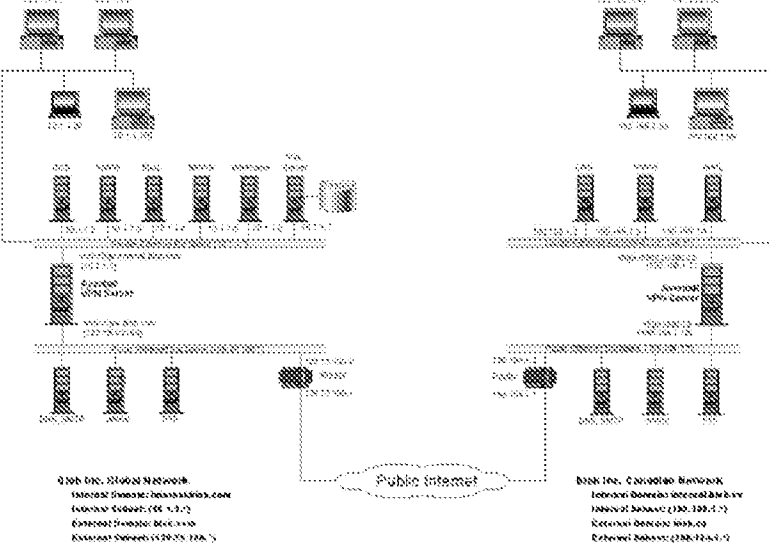
MULTIPROXY: The user authenticates with server2 directly.





 **Authenticated and encrypted tunnel**
 In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.

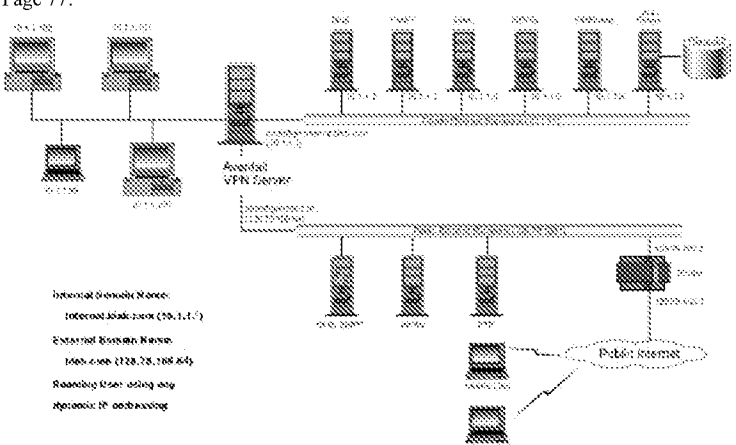
Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.

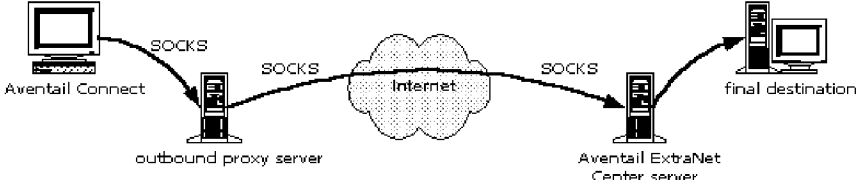
Page 79:

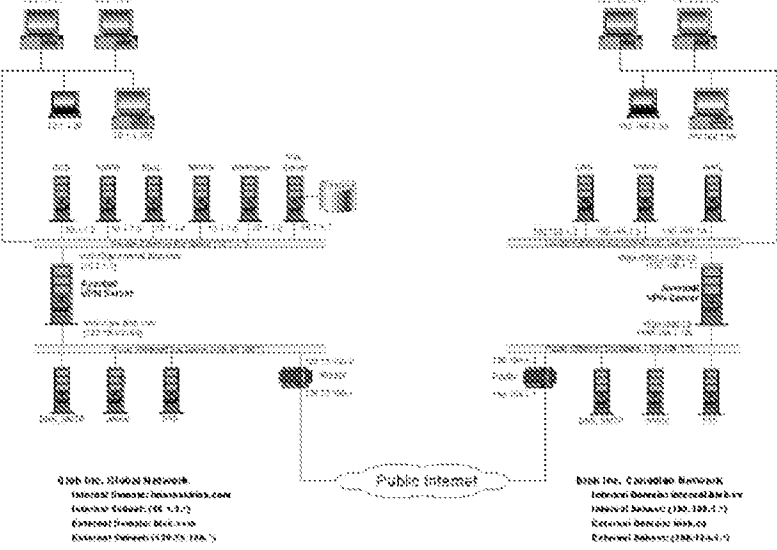
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p>
<p>receiving a secure domain name;</p>	<p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p> <p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
<p>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <ul style="list-style-type: none"> • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. <p>Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution.</p> <p>Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.</p>
<p>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <ul style="list-style-type: none"> • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet.</p> <p>Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically.</p> <p>Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.</p> <p>Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.</p> <p>Page 69: The client application requests access to the destination server.</p> <p>Page 72:</p> <p>PROXY CHAINING: Server1 appears as a user to server2.</p>  <p>MULTIPROXY: The user authenticates with server2 directly.</p>  <div data-bbox="552 1281 958 1417" style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">↔ Authenticated and encrypted tunnel</p> <p>In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.</p> </div> <p>Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.</p> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will</p>




7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p> <p>Page 77:</p>  <p>Internal Machine Name: 10000130ak.2000 (20.1.1.1)</p> <p>Internal Machine Name: 1000.000 (128.78.108.64)</p> <p>Routing User: 0000.000</p> <p>Automatic IP: 0000.000</p> <p>Example Corporate Network Design using Mobile VPN</p> <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p> <p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p>
<p>20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 68: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server.</p> <p>The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination.</p>

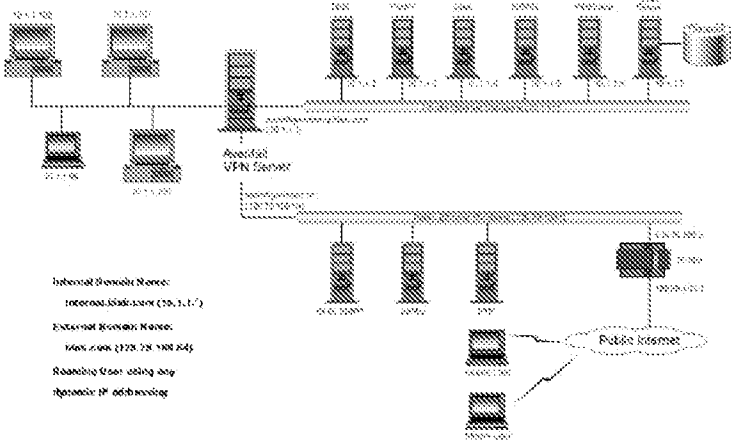
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>Any or all of the proxy servers can apply authentication and access control rules.</p> <p>Page 69: In the following diagram, the Aventail ExtraNet Server acts as both a destination and a server. It is a destination because a proxy server routes traffic to it. It is a server because it routes traffic to the final destination.</p>  <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p>
<p>26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.</p>	<p>Page 5: Aventail Corporation is the leading vendor of extranet software. Its extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet.</p> <p>Page 8: Windows TCP/IP networking applications (such as telnet, e-mail, Web browsers, and ftp) use WinSock to gain access to networks or the Internet. WinSock is the core component of TCP/IP under Windows, and is the interface that most Windows applications use to communicate to TCP/IP.</p> <p>Page 79:</p>




7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p>
<p>28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet.</p> <p>Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.</p> <p>Pages 12-13: When the SOCKS negotiation is completed, Aventail Connect notifies the application. Form the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the</p>

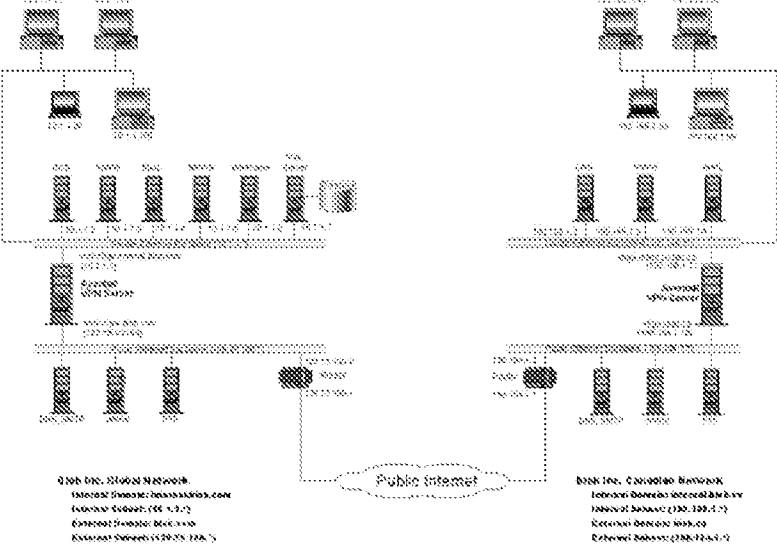
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>TCP handshaking.</p> <p>Page 69: Once the connection between the client and the Aventail ExtraNet Server is established, the output server simply relays the data.</p> <p>Page 69: The client application requests access to the destination server.</p> <p>Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.</p>
<p>29. The computer-readable medium according to claim 17,</p>	
<p>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.</p>
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <ul style="list-style-type: none"> • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. <p>Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution.</p> <p>Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.</p>
<p>wherein receiving the response</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
<p>message comprises receiving the response message at the client computer,</p>	<p>Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>• If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.</p> <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet.</p> <p>Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically.</p> <p>Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.</p> <p>Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.</p> <p>Page 69: The client application requests access to the destination server.</p> <p>Page 72:</p>

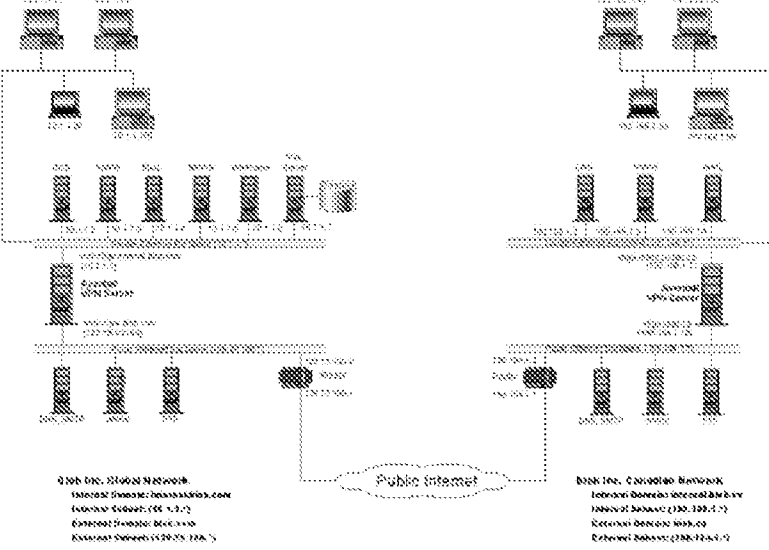
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>PROXY CHAINING: Server1 appears as a user to server2.</p>  <p>MULTIPROXY: The user authenticates with server2 directly.</p>  <div data-bbox="560 1029 966 1155" style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">  Authenticated and encrypted tunnel </p> <p>In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.</p> </div> <p>Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.</p> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p> <p>Page 77:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p>Example Corporate Network Design using Mobile VPN</p> <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p> <p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p>
<p>30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.</p>	<p>See claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer).</p>
<p>31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.</p>	<p>See claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer). Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the user's desktop.</p>
<p>33. A data processing apparatus, comprising:</p>	<p>Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files.</p>



7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location.</p> <p>Page 72:</p> <p>PROXY CHAINING: Server1 appears as a user to server2.</p>  <p>MULTIPROXY: The user authenticates with server2 directly.</p>  <div data-bbox="552 1123 966 1260" style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">  Authenticated and encrypted tunnel </p> <p style="font-size: small;">In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.</p> </div> <p>Page 79:</p>

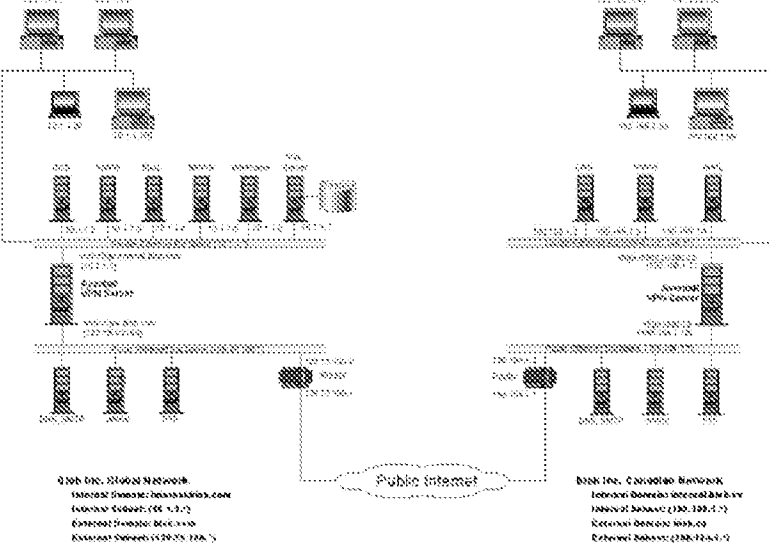
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference								
	 <p data-bbox="698 1176 1128 1197">Example Corporate Network Design using Partner VPN</p>								
a processor, and	<p data-bbox="516 1228 592 1249">Page 13:</p> <p data-bbox="516 1255 998 1281">Aventail Connect Platform Requirements</p> <p data-bbox="552 1285 1291 1333">The following table lists the minimum system requirements for each of the platforms that Aventail Connect supports.</p> <table border="1" data-bbox="568 1354 1226 1491"> <thead> <tr> <th>Platform</th> <th>Processor</th> <th>RAM</th> <th>SOCKS Server</th> </tr> </thead> <tbody> <tr> <td>windows 98; Windows NT 4.0 (requires Microsoft Service Pack 3 or above)</td> <td>x86-based or Pentium personal computer</td> <td>16 MB</td> <td>Network-accessible SOCKS v4 or v5 compliant server</td> </tr> </tbody> </table>	Platform	Processor	RAM	SOCKS Server	windows 98; Windows NT 4.0 (requires Microsoft Service Pack 3 or above)	x86-based or Pentium personal computer	16 MB	Network-accessible SOCKS v4 or v5 compliant server
Platform	Processor	RAM	SOCKS Server						
windows 98; Windows NT 4.0 (requires Microsoft Service Pack 3 or above)	x86-based or Pentium personal computer	16 MB	Network-accessible SOCKS v4 or v5 compliant server						

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference			
	Windows 95; Windows NT 3.51	x86-based or Pentium personal computer	8 MB	Network-accessible SOCKS v4 or v5 compliant server
	Windows 3.1; Windows for Workgroups 3.11	x86-based or Pentium personal computer	4 MB	Network-accessible SOCKS v4 or v5 compliant server
<p>Aventail Connect 3.1 runs on the following operating systems: Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files. Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location. Page 79:</p>				



7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p>
<p>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. The first response to these concerns has been the development of security firewalls—software barriers that control the flow of information. But firewalls are not designed to handle complex security issues, such as monitoring network usage, providing private communication over public networks, and enabling remote users to gain secure access to internal network resources.</p> <p>Page 12: b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.</p> <ul style="list-style-type: none"> • It sends the list of authentication methods enabled in the configuration file • Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. • It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address

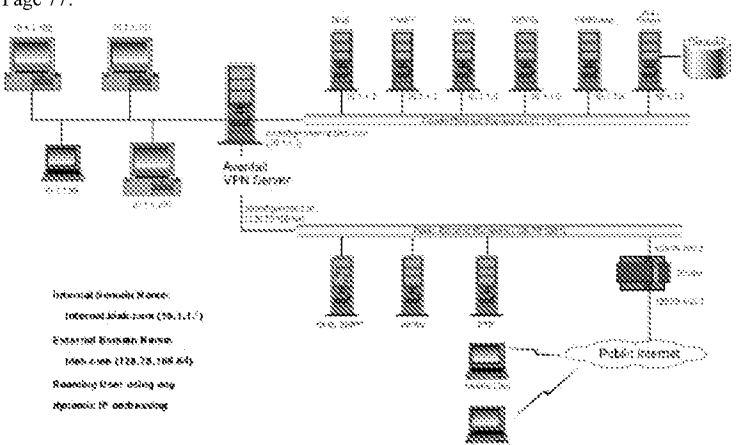
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>provided by the application or the DNS entry (hostname) provided in step 1.</p> <p>Page 46: SOCKS v5 servers often require user authentication before allowing access. Aventail Connect authentication modules display dialog boxes that prompt users to enter username and password information as well as other authentication credentials.</p> <p>The current Aventail Connect authentication modules are SOCKS v4 Identification, Username / Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password).</p> <p>Page 62: Once servers and destinations are defined, you can direct SOCKS traffic through successive extranet (SOCKS) servers.</p> <p>Page 66: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. This capability is provided in Aventail Connect 3.1 by the Aventail MultiProxy feature. Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining.</p> <p>Page 72:</p>

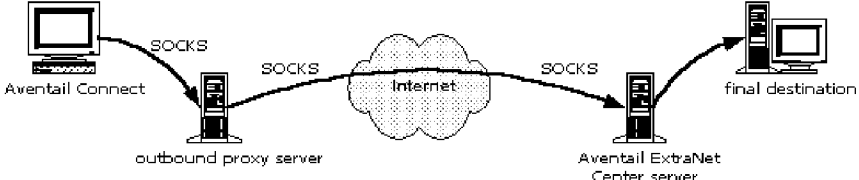
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>PROXY CHAINING: Server1 appears as a user to server2.</p>  <p>MULTIPROXY: The user authenticates with server2 directly.</p>  <div data-bbox="560 1029 966 1165" style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">↔ Authenticated and encrypted tunnel</p> <p>In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.</p> </div> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p> <p>Page 79:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 <p style="text-align: center;">Example Corporate Network Design using Partner VPN</p> <p>Bob Inc. Global Network Internet Gateway: bobincglobal.com Corporate Gateway: 10.1.1.1 Corporate DNS: 10.1.1.2 Corporate Server: 10.1.1.3</p> <p>Bob Inc. Global Network Internet Gateway: bobincglobal.com Corporate Gateway: 10.1.1.1 Corporate DNS: 10.1.1.2 Corporate Server: 10.1.1.3</p> <p style="text-align: center;">Public Internet</p>
receiving a secure domain name;	<p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p> <p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.</p> <p>Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.</p>

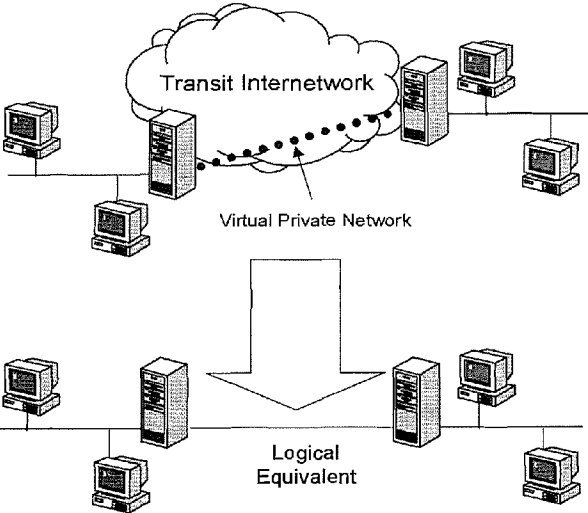
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <ul style="list-style-type: none"> • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. <p>Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution.</p> <p>Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.</p>
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.</p> <p>Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution.</p> <ul style="list-style-type: none"> • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet.</p> <p>Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically.</p> <p>Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.</p> <p>Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.</p> <p>Page 69: The client application requests access to the destination server.</p> <p>Page 72:</p> <p>PROXY CHAINING: Server1 appears as a user to server2.</p>  <p>MULTIPROXY: The user authenticates with server2 directly.</p>  <div data-bbox="552 1281 958 1417" style="border: 1px solid black; padding: 5px;"> <p>↔ Authenticated and encrypted tunnel</p> <p>In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.</p> </div> <p>Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.</p> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will</p>

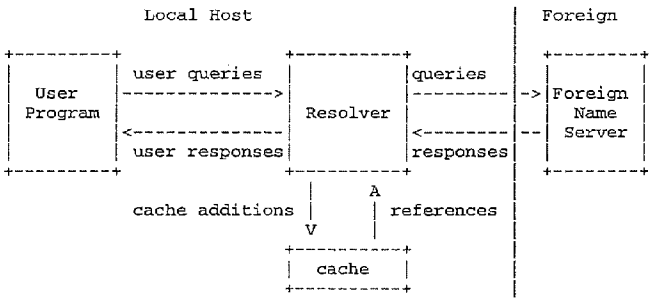
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p> <p>Page 77:</p>  <p>Internal Machine Name: 10000136ak2300 (20.11.1.1)</p> <p>Internal Machine Name: 1000-4300 (128.78.168.64)</p> <p>Routing User: 02000-000</p> <p>Automatic IP: 000000000</p> <p>Example Corporate Network Design using Mobile VPN</p> <p>Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.</p> <p>Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.</p>
<p>35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 68: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server.</p> <p>The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination.</p>

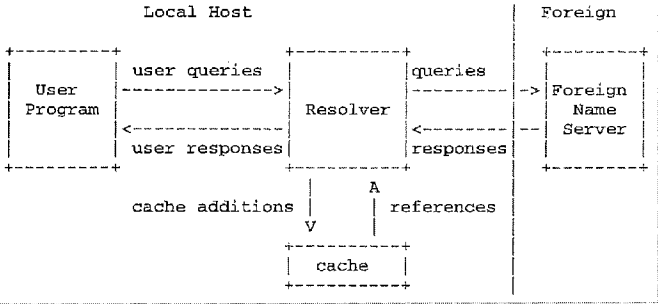
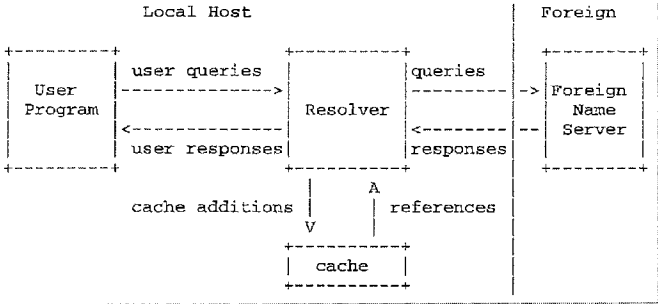
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	<p>Any or all of the proxy servers can apply authentication and access control rules.</p> <p>Page 69: In the following diagram, the Aventail ExtraNet Server acts as both a destination and a server. It is a destination because a proxy server routes traffic to it. It is a server because it routes traffic to the final destination.</p>  <p>The diagram illustrates a network path. On the left, a computer icon labeled 'Aventail Connect' is connected via a 'SOCKS' arrow to a server icon labeled 'outbound proxy server'. From the 'outbound proxy server', another 'SOCKS' arrow points to a cloud icon labeled 'Internet'. From the 'Internet', a 'SOCKS' arrow points to a server icon labeled 'Aventail ExtraNet Center server'. Finally, an arrow points from the 'Aventail ExtraNet Center server' to a computer icon labeled 'final destination'.</p> <p>Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.</p>

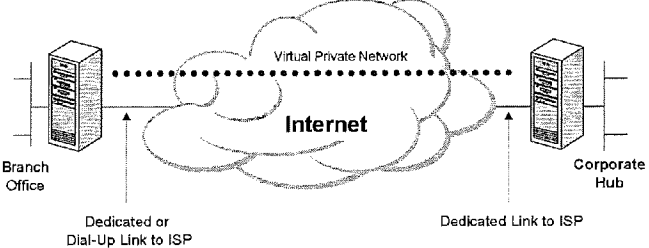
Appendix B
Citations to Exemplary Description in the VPN Overview and RFC 1035 References*

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to <i>tunnel</i> through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).</p>  <p align="center"><i>Figure 1: Virtual Private Network</i></p> <p>VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate</p>

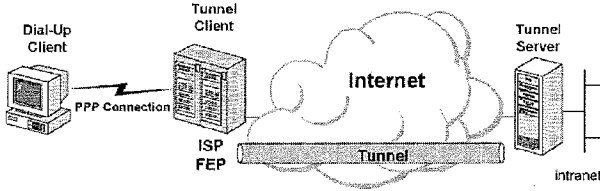
* - The cited passages are an indication of where in the VPN Overview and RFC 1035 references, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.</p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p>
receiving a secure domain name;	<p>VPN Overview, Page 26: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses.</p> <p>RFC 1035, Page 4:</p>  <pre> sequenceDiagram participant User as User Program participant Resolver participant Foreign as Foreign Name Server participant Cache as cache User->>Resolver: user queries Resolver->>Foreign: queries Foreign-->>Resolver: responses Resolver-->>User: user responses Resolver-->>Cache: cache additions V Cache-->>Resolver: references A </pre>
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet).</p> <p>VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.</p> <p>RFC 1035, Page 4:</p>

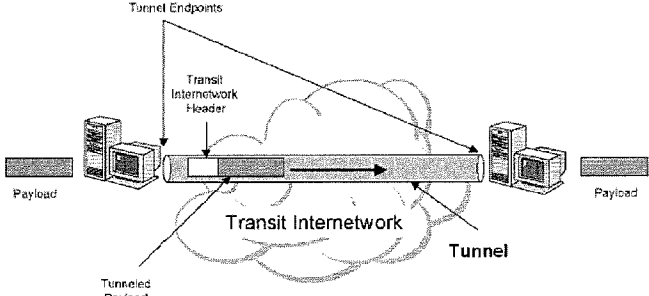
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>RFC 1035, Page 4:</p> 
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet).</p> <p>VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.</p> <p>VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.</p>

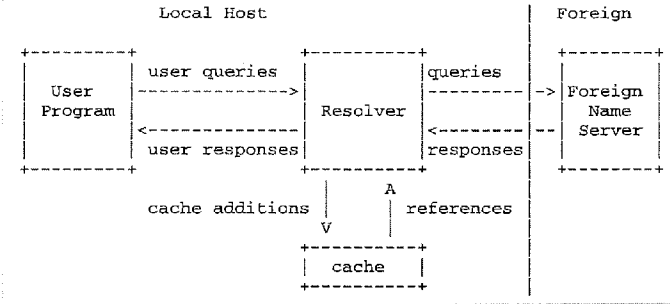
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <p data-bbox="565 909 927 930"><i>Figure 3: Using a VPN to connect two remote sites</i></p> <p data-bbox="565 961 1446 1077">VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p data-bbox="565 1081 1425 1125">User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p data-bbox="565 1129 1442 1245">VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork.</p> <p data-bbox="565 1249 771 1270">VPN Overview, Page 10:</p>

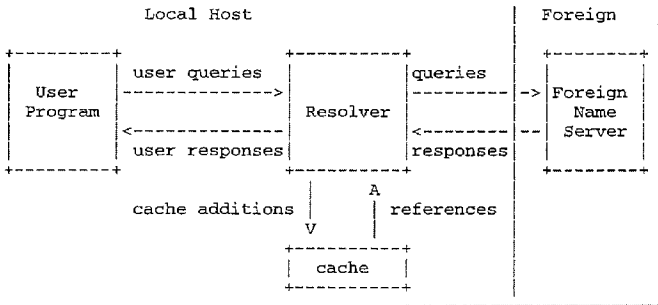
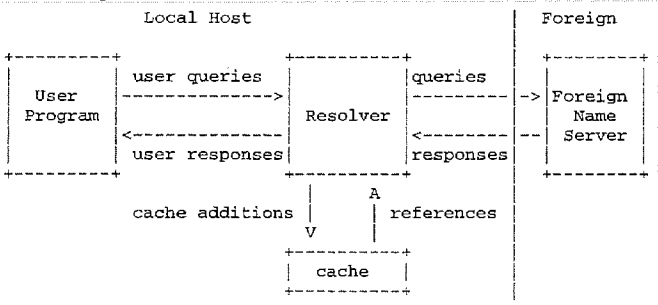
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<div data-bbox="662 640 1307 955" data-label="Diagram"> <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown as a small rectangular block. This payload is combined with a 'Transit Internet Header' to form a 'Tunneled Payload', represented as a larger rectangular block. This tunneled payload is then sent through a 'Tunnel' (represented by a horizontal arrow) across a 'Transit Internet Network' (represented by a cloud). The tunnel terminates at 'Tunnel Endpoints' on the right, where the tunneled payload is decapsulated to retrieve the original 'Payload'.</p> </div> <p data-bbox="665 976 803 997"><i>Figure 5: Tunneling</i></p> <p data-bbox="560 1029 1453 1186">VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.</p> <p data-bbox="560 1192 1453 1239">VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p data-bbox="560 1245 1453 1312">VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation.</p> <p data-bbox="560 1318 1453 1428">VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p data-bbox="560 1434 1453 1501">VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with an ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to</p>

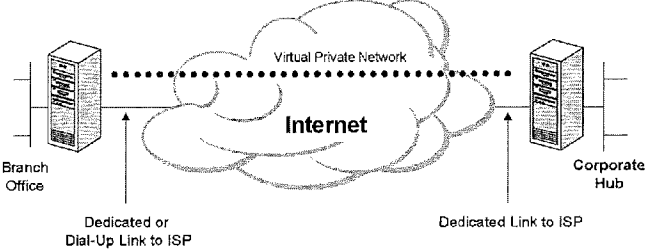
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network. VPN Overview, Page 22:</p>  <p style="text-align: center;"><i>Figure 9: Compulsory tunneling</i></p> <p>VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p>VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication--despite the fact that this communication occurs over a public internetwork.</p>
<p>4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.</p>	<p>VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<div data-bbox="592 640 1242 892" data-label="Diagram"> </div> <p data-bbox="560 907 922 928"><i>Figure 3: Using a VPN to connect two remote sites</i></p> <p data-bbox="560 938 1445 1054">VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p data-bbox="560 1056 1424 1100">User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p data-bbox="560 1102 1406 1146">VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p data-bbox="560 1148 1455 1266">VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p data-bbox="560 1268 1455 1409">VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p data-bbox="560 1411 1455 1501">VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication--despite the fact that this communication occurs over a public internetwork.</p>

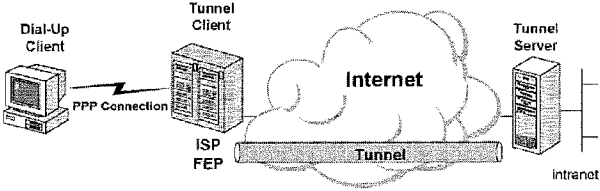
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
<p>10. The method according to claim 1, wherein the virtual private network includes the Internet.</p>	<p>VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to <i>tunnel</i> through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1). VPN Overview, Page 10:</p>  <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown. This payload is encapsulated into a 'Tunnelled Payload' (represented by a box with a double arrow). This tunnelled payload is then sent through a 'Tunnel' (represented by a long arrow) that passes through a 'Transit Internetwork' (represented by a cloud). The tunnel is bounded by 'Tunnel Endpoints' (represented by computer icons). A 'Transit Internetwork Header' is also shown as part of the tunnel structure.</p> <p>Figure 5: Tunneling</p>
<p>12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly. VPN Overview, Page 16: Once the four phases of negotiation have been completed, PPP begins to forward</p>

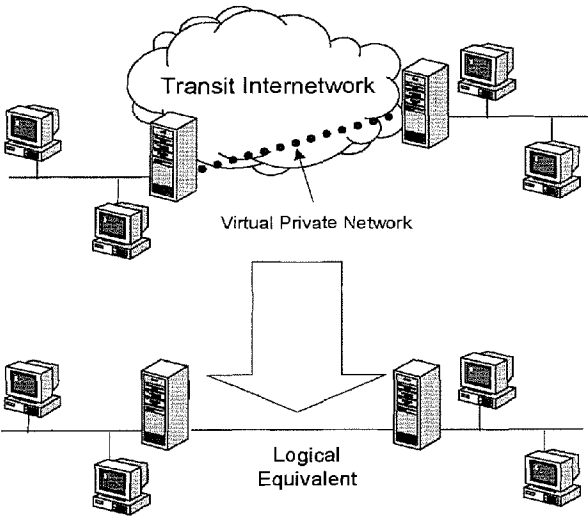
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>data to and from the two peers. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p>
13. The method of claim 1,	
<p>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>RFC 1035, Page 4:</p>  <pre> sequenceDiagram participant User as User Program participant Resolver participant Foreign as Foreign Name Server User->>Resolver: user queries Resolver->>Foreign: queries Foreign-->>Resolver: responses Resolver-->>User: user responses Note over Resolver: cache additions Note over Resolver: references Note over Resolver: cache </pre>
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>RFC 1035, Page 4:</p>

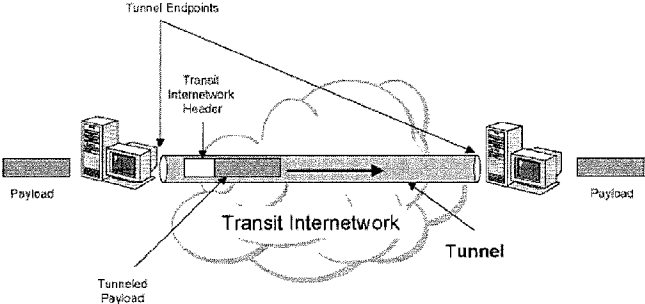
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <pre> sequenceDiagram participant UP as User Program participant R as Resolver participant FNS as Foreign Name Server participant C as cache UP->>R: user queries R-->>UP: user responses R->>FNS: queries FNS-->>R: responses R->>C: cache additions V C-->>R: references A </pre>
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>RFC 1035, Page 4:</p>  <pre> sequenceDiagram participant UP as User Program participant R as Resolver participant FNS as Foreign Name Server participant C as cache UP->>R: user queries R-->>UP: user responses R->>FNS: queries FNS-->>R: responses R->>C: cache additions V C-->>R: references A </pre>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet).</p> <p>VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.</p> <p>VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.</p>

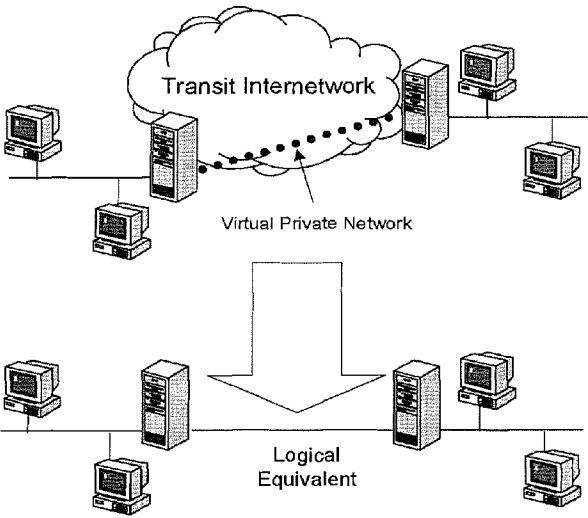
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <p data-bbox="565 909 925 930"><i>Figure 3: Using a VPN to connect two remote sites</i></p> <p data-bbox="565 940 1445 1056">VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p data-bbox="565 1060 1421 1102">User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p data-bbox="565 1106 1437 1224">VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork.</p> <p data-bbox="565 1228 771 1249">VPN Overview, Page 10:</p>

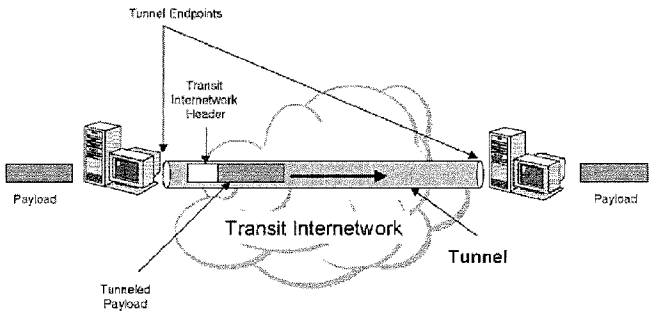
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<div data-bbox="662 640 1307 955" data-label="Diagram"> <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown as a small rectangular block. This payload is combined with a 'Tunnel Header' to form a 'Tunneled Payload', represented as a larger rectangular block. This tunneled payload is then sent through a 'Transit Internetwork', depicted as a cloud. The path through the cloud is labeled 'Tunnel'. On the right side of the cloud, the tunneled payload is received at a 'Tunnel Endpoint'. The endpoint then extracts the original 'Payload' from the tunneled payload. Labels include 'Payload', 'Tunnel Header', 'Tunneled Payload', 'Transit Internetwork', and 'Tunnel Endpoints'.</p> </div> <p data-bbox="665 976 803 997"><i>Figure 5: Tunneling</i></p> <p data-bbox="560 1003 1437 1165">VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.</p> <p data-bbox="560 1165 1437 1207">VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p data-bbox="560 1207 1437 1270">VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation.</p> <p data-bbox="560 1270 1437 1396">VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p data-bbox="560 1396 1437 1480">VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with an ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a</p>

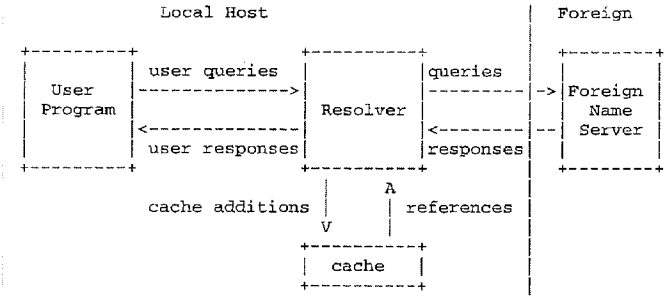
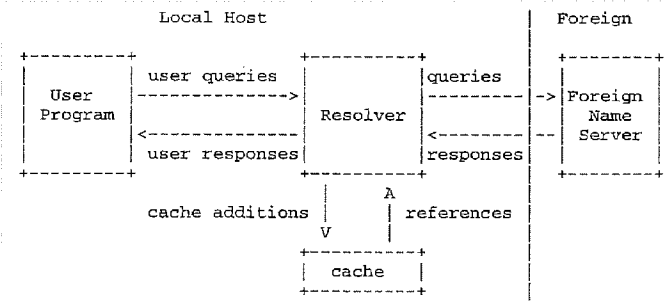
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>single Internet connection at the corporate network. VPN Overview, Page 22:</p>  <p style="text-align: center;"><i>Figure 9: Compulsory tunneling</i></p> <p>VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p>VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication--despite the fact that this communication occurs over a public internetwork.</p>
14. The method of claim 1, performed by a software module.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer.
15. The method of claim 1, performed by a client computer.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer. VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to <i>tunnel</i> through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).

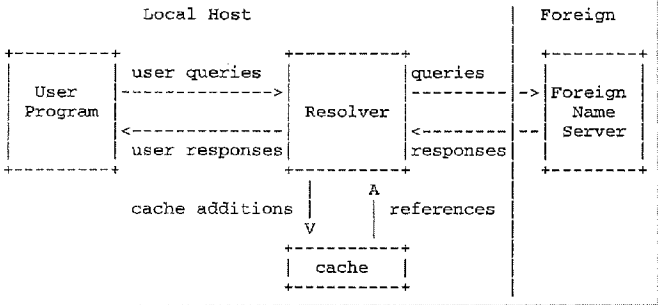
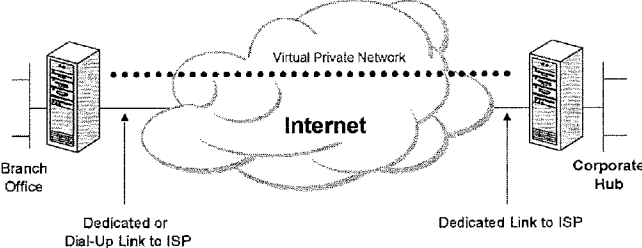
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <p>The diagram illustrates the concept of a Virtual Private Network (VPN). At the top, a cloud labeled 'Transit Internetwork' contains several server icons. Below it, a 'Virtual Private Network' is shown as a series of dots connected by a line, representing a secure tunnel through the transit network. A large downward-pointing arrow indicates the logical equivalence between the VPN and a direct connection. At the bottom, the 'Logical Equivalent' is shown as a direct point-to-point connection between a user's computer and a corporate server, bypassing the transit network.</p> <p><i>Figure 1: Virtual Private Network</i></p> <p>VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.</p>
17. A computer-readable storage medium, comprising:	VPN Overview, Page 10:

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown. This payload is encapsulated into a 'Tunnelled Payload' which is then sent through a 'Tunnel' that spans across a 'Transit Internetwork' (represented by a cloud). The tunnel is bounded by 'Tunnel Endpoints'. A 'Transit Internetwork Header' is added to the tunnelled payload before it enters the tunnel. On the right, the tunnel ends at another endpoint, where the 'Tunnelled Payload' is decapsulated back into the original 'Payload'.</p> <p><i>Figure 5: Tunneling</i></p> <p>VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.</p>
a storage area; and	VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to <i>tunnel</i> through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <p>The diagram illustrates a Virtual Private Network (VPN) setup. At the top, a cloud labeled "Transit Internetwork" contains several server icons. Below the cloud, a dashed line represents the "Virtual Private Network" connecting two specific server icons. A large downward-pointing arrow indicates a transition to a "Logical Equivalent" network at the bottom, which shows a direct connection between the two server icons, bypassing the transit internetwork. The entire diagram is surrounded by various computer and server icons representing network participants.</p> <p><i>Figure 1: Virtual Private Network</i></p> <p>VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.</p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized</p>

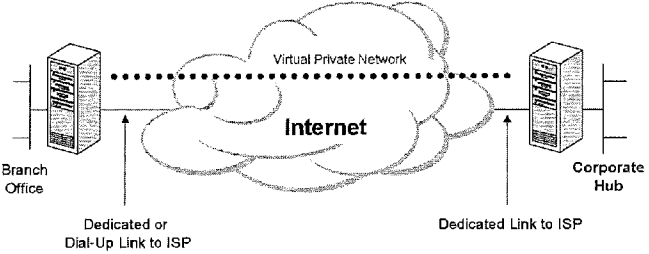
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>users only. VPN Overview, Page 10:</p>  <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown. This payload is encapsulated into a 'Tunnel' structure. The tunnel consists of a 'Tunnel Header' and a 'Tunneled Payload'. This tunnel is then sent through a 'Transit Internet Network' (represented by a cloud) to 'Tunnel Endpoints' on the right. The endpoints then extract the original 'Payload'.</p> <p><i>Figure 5: Tunneling</i></p> <p>VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.</p>
<p>receiving a secure domain name;</p>	<p>VPN Overview, Page 26: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses.</p> <p>RFC 1035, Page 4:</p>

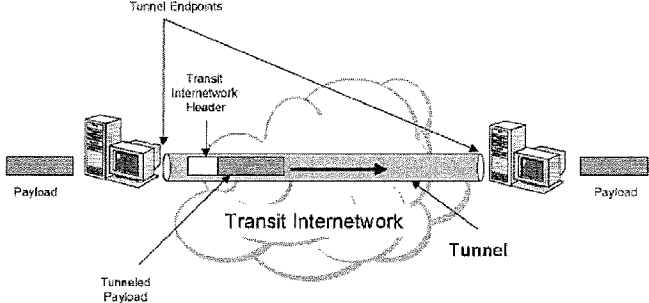
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <pre> sequenceDiagram participant User as User Program participant Resolver participant Foreign as Foreign Name Server participant Cache as cache User->>Resolver: user queries Resolver->>Foreign: queries Foreign-->>Resolver: responses Resolver-->>User: user responses Resolver->>Cache: cache additions (V) Cache-->>Resolver: references (A) </pre>
<p>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet).</p> <p>VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.</p> <p>RFC 1035, Page 4:</p>  <pre> sequenceDiagram participant User as User Program participant Resolver participant Foreign as Foreign Name Server participant Cache as cache User->>Resolver: user queries Resolver->>Foreign: queries Foreign-->>Resolver: responses Resolver-->>User: user responses Resolver->>Cache: cache additions (V) Cache-->>Resolver: references (A) </pre>
<p>receiving from the domain name service a response message containing the secure computer network address</p>	<p>RFC 1035, Page 4:</p>

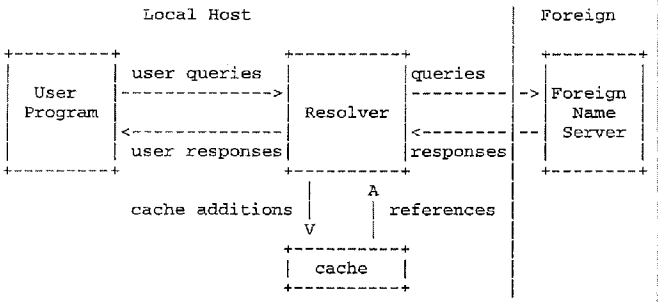
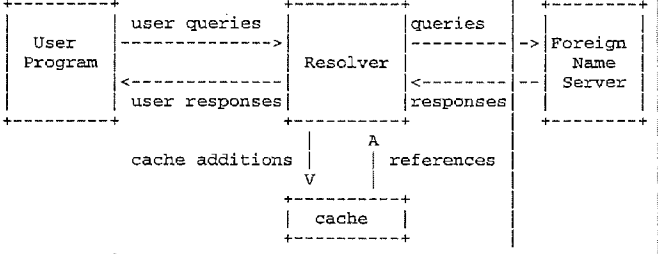
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
<p>corresponding to the secure domain name; and</p>	 <pre> sequenceDiagram participant UP as User Program participant R as Resolver participant FNS as Foreign Name Server participant C as cache UP->>R: user queries R->>FNS: queries FNS-->>R: responses R-->>UP: user responses R-->>C: cache additions C-->>R: references </pre>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet).</p> <p>VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.</p> <p>VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.</p>  <p><i>Figure 3: Using a VPN to connect two remote sites</i></p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p>VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork.</p> <p>VPN Overview, Page 10:</p> <div data-bbox="662 905 1307 1213" data-label="Diagram"> <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown as a rectangular block. This payload is combined with a 'Transit Internetwork Header' to form a 'Tunneled Payload', represented as a larger rectangular block with an arrow pointing right. This tunneled payload is sent through a 'Tunnel' (represented by a cloud-like shape) across a 'Transit Internetwork'. The tunnel is bounded by 'Tunnel Endpoints' at both ends. On the right side, the tunneled payload is received and the original 'Payload' is extracted.</p> </div> <p><i>Figure 5: Tunneling</i></p> <p>VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.</p> <p>VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p>VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation.</p> <p>VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p>VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with an ISP to deploy a nationwide set of FEPs. These <u>FEPs can establish tunnels across the Internet</u> to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network.</p> <p>VPN Overview, Page 22:</p> <div data-bbox="667 961 1268 1157" data-label="Diagram"> <p>The diagram illustrates the compulsory tunneling process. On the left, a 'Dial-Up Client' (represented by a computer monitor) is connected via a 'PPP Connection' to an 'ISP FEP' (Internet Service Provider Front-End Processor). From the 'ISP FEP', the connection goes to a 'Tunnel Client' located on the 'Internet' (represented by a cloud). The 'Tunnel Client' then connects to a 'Tunnel Server' located on an 'intranet'. A 'Tunnel' is shown as a path through the Internet cloud connecting the Tunnel Client and the Tunnel Server.</p> </div> <p>Figure 9: Compulsory tunneling</p> <p>VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p>VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication--despite the fact that this communication occurs over a public internetwork.</p>
20. The computer-readable medium	VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
<p>according to claim 17, wherein the response message contains provisioning information for the virtual private network.</p>	<p>network between the branch office router and the corporate hub router across the Internet.</p>  <p><i>Figure 3: Using a VPN to connect two remote sites</i></p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p>VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p>VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p>VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p>VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	communication-despite the fact that this communication occurs over a public internetwork.
<p>26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.</p>	<p>VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to <i>tunnel</i> through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).</p> <p>VPN Overview, Page 10:</p>  <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown. This payload is encapsulated into a 'Tunneled Payload' which is then sent through a 'Tunnel' that exists within a 'Transit Internetwork' (represented by a cloud). The tunnel is bounded by 'Tunnel Endpoints'. A 'Transit Internetwork Header' is added to the tunneled payload before it enters the tunnel. On the right side, the tunneled payload is received and the original 'Payload' is extracted.</p> <p>Figure 5: Tunneling</p>
<p>28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.</p> <p>VPN Overview, Page 16: Once the four phases of negotiation have been completed, PPP begins to forward data to and from the two peers.</p> <p>VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer</p>

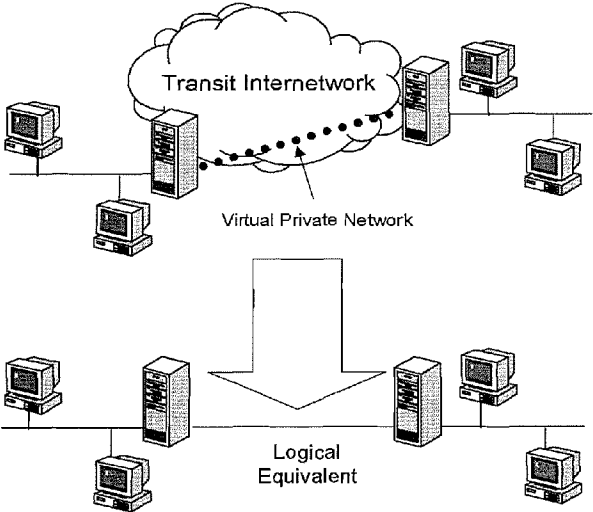
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.
<p>29. The computer-readable medium according to claim 17, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>RFC 1035, Page 4:</p>  <pre> sequenceDiagram participant User as User Program participant Resolver participant Foreign as Foreign Name Server participant cache User->>Resolver: user queries Resolver->>Foreign: queries Foreign-->>Resolver: responses Resolver-->>User: user responses Resolver->>cache: cache additions (V) cache-->>Resolver: references (A) </pre>
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>RFC 1035, Page 4:</p>  <pre> sequenceDiagram participant User as User Program participant Resolver participant Foreign as Foreign Name Server participant cache User->>Resolver: user queries Resolver->>Foreign: queries Foreign-->>Resolver: responses Resolver-->>User: user responses Resolver->>cache: cache additions (V) cache-->>Resolver: references (A) </pre>
<p>wherein receiving the response</p>	<p>RFC 1035, Page 4:</p>

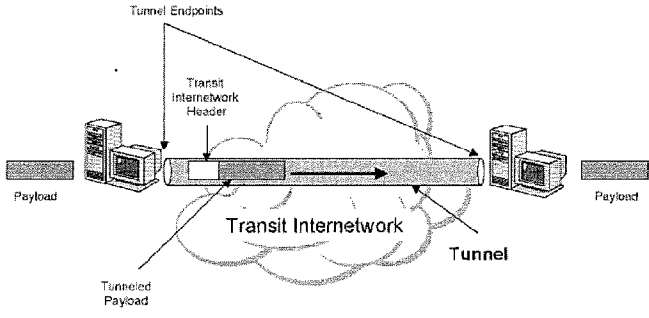
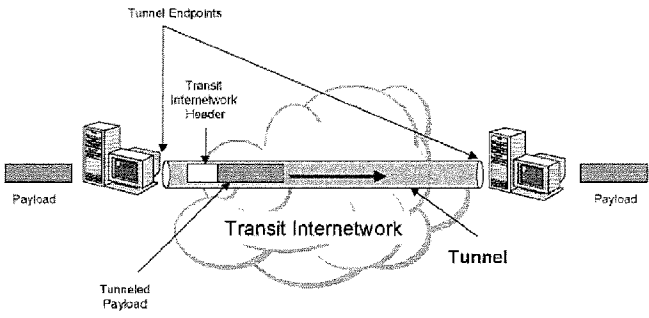
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
<p>message comprises receiving the response message at the client computer,</p>	<pre> sequenceDiagram participant UP as User Program participant R as Resolver participant FNS as Foreign Name Server participant C as cache UP->>R: user queries R-->>UP: user responses R->>FNS: queries FNS-->>R: responses R-->>C: cache additions C-->>R: references </pre>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet).</p> <p>VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.</p> <p>VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.</p> <p style="text-align: center;">Figure 3: Using a VPN to connect two remote sites</p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the</p>

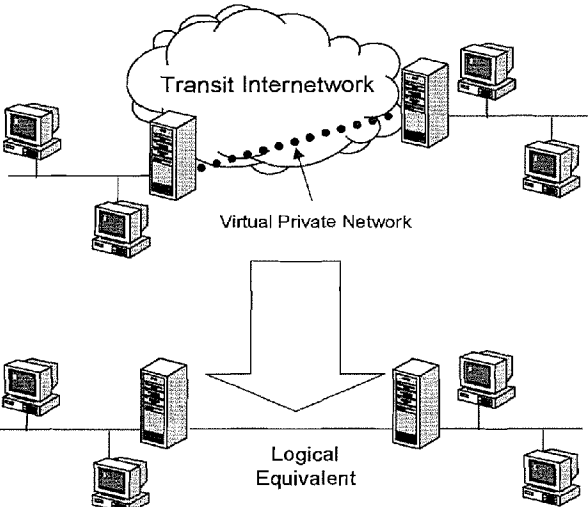
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p>VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork.</p> <p>VPN Overview, Page 10:</p> <div data-bbox="662 949 1307 1260" data-label="Diagram"> <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown as a small rectangular block. This payload is combined with a 'Transit Internet Network Header' to form a 'Tunnelled Payload', represented as a larger rectangular block with an arrow pointing right. This tunnelled payload is sent through a 'Tunnel' (represented by a cloud-like shape) across a 'Transit Internetwork' (represented by a larger cloud-like shape). On the right, the tunnelled payload is received at a 'Tunnel Endpoint' and the original 'Payload' is extracted. Labels include 'Payload', 'Transit Internet Network Header', 'Tunnelled Payload', 'Transit Internetwork', 'Tunnel', and 'Tunnel Endpoints'.</p> </div> <p><i>Figure 5: Tunneling</i></p> <p>VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.</p>

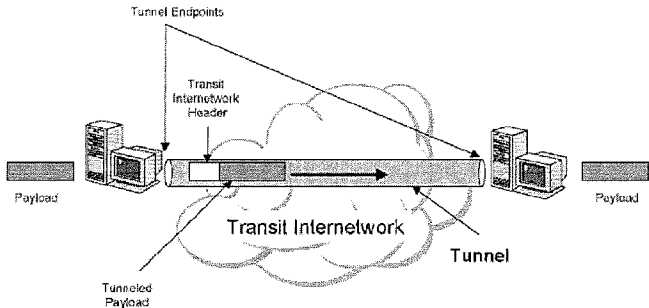
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p>VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation.</p> <p>VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p>VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with an ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network.</p> <p>VPN Overview, Page 22:</p> <div data-bbox="667 1037 1268 1224" data-label="Diagram"> <p>The diagram illustrates the compulsory tunneling process. On the left, a 'Dial-Up Client' (represented by a computer monitor) is connected to an 'ISP FEP' (Tunnel Client) via a 'PPP Connection'. The 'ISP FEP' is connected to the 'Internet' (represented by a cloud). The 'Internet' is connected to a 'Tunnel Server', which is in turn connected to an 'intranet'. A 'Tunnel' is shown as a shaded bar between the 'ISP FEP' and the 'Tunnel Server'.</p> </div> <p>Figure 9: Compulsory tunneling</p> <p>VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p>VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network</p>

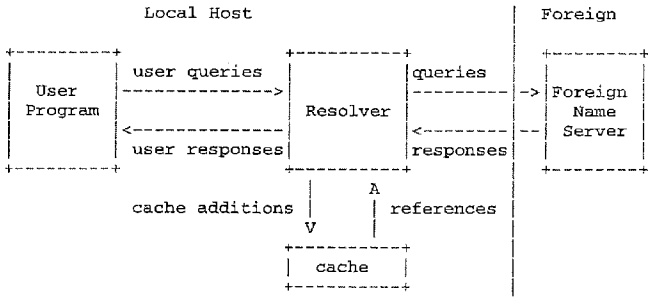
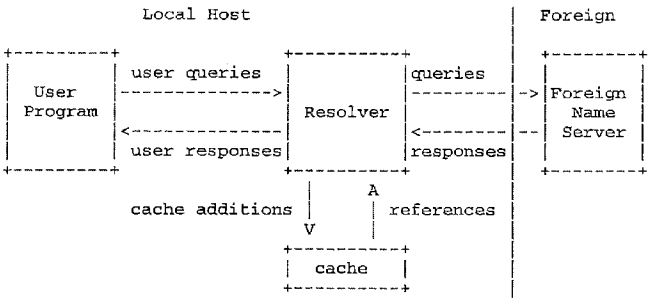
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	communication-despite the fact that this communication occurs over a public internetwork.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer.
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer. VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to <i>tunnel</i> through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).

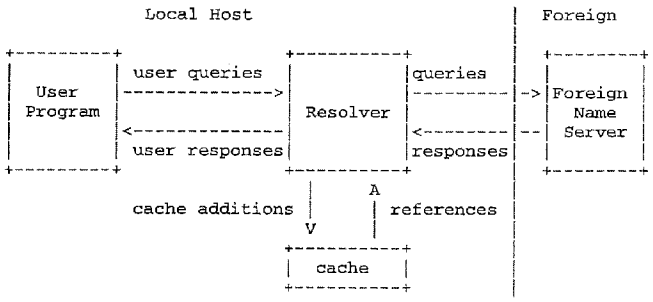
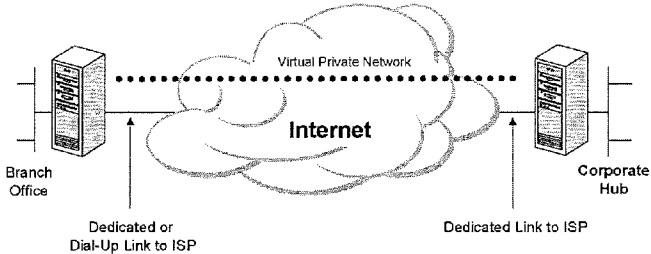
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <p>The diagram illustrates a Virtual Private Network (VPN) setup. At the top, a cloud labeled 'Transit Internetwork' contains several server icons and a dotted line representing a network path. Below this, a 'Virtual Private Network' is shown as a point-to-point connection between two server icons. A large downward-pointing arrow indicates a transition to a 'Logical Equivalent' network at the bottom, which also shows a point-to-point connection between two server icons. The diagram uses icons for desktop computers and server racks to represent network nodes.</p> <p><i>Figure 1: Virtual Private Network</i></p> <p>VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.</p>
33. A data processing apparatus, comprising:	VPN Overview, Page 10:

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown as a rectangular block. This payload is encapsulated into a 'Tunnel' structure, which includes a 'Tunnel Endpoint' at the start and a 'Tunnel Endpoint' at the end. The tunnel is shown as a long horizontal bar with an arrow pointing from left to right. The tunnel is labeled 'Tunnel' at its right end. The tunnel is shown passing through a cloud-like shape labeled 'Transit Internetwork'. The payload inside the tunnel is labeled 'Tunneled Payload'. A 'Transit Internetwork Header' is shown as a small rectangular block at the beginning of the tunnel. The diagram is labeled 'Figure 5: Tunneling'.</p> <p><i>Figure 5: Tunneling</i> VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.</p>
a processor, and	 <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown as a rectangular block. This payload is encapsulated into a 'Tunnel' structure, which includes a 'Tunnel Endpoint' at the start and a 'Tunnel Endpoint' at the end. The tunnel is shown as a long horizontal bar with an arrow pointing from left to right. The tunnel is labeled 'Tunnel' at its right end. The tunnel is shown passing through a cloud-like shape labeled 'Transit Internetwork'. The payload inside the tunnel is labeled 'Tunneled Payload'. A 'Transit Internetwork Header' is shown as a small rectangular block at the beginning of the tunnel. The diagram is labeled 'Figure 5: Tunneling'.</p> <p><i>Figure 5: Tunneling</i> VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.</p>
memory storing computer executable	VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
<p>instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>another network. VPNs accomplish this by allowing the user to <i>tunnel</i> through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).</p>  <p>The diagram illustrates the concept of a Virtual Private Network (VPN). It is divided into two parts. The top part shows a 'Transit Internetwork' represented by a cloud containing several server icons. A 'Virtual Private Network' is shown as a series of dots connected by a line, tunneling through the Transit Internetwork. The bottom part shows a 'Logical Equivalent' network, which appears as a direct connection between a user's computer and a corporate server, bypassing the public network. A large downward-pointing arrow connects the two parts, indicating the transition from the actual network state to the user's logical perspective.</p> <p><i>Figure 1: Virtual Private Network</i></p> <p>VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.</p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the</p>

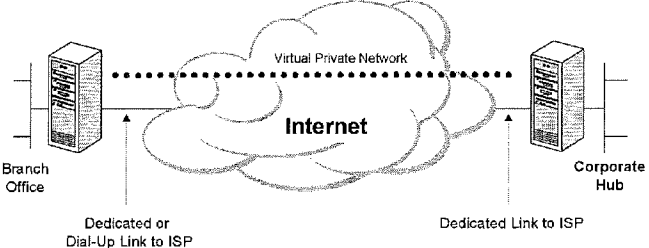
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p>VPN Overview, Page 10:</p>  <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown. This payload is encapsulated into a 'Tunnel' structure. The 'Tunnel' consists of a 'Transit Internetwork Header' and a 'Tunnel' body. The 'Tunnel' body contains the 'Tunneled Payload'. The 'Tunnel' is sent through a 'Transit Internetwork' (represented by a cloud) to 'Tunnel Endpoints' on the right. At the right endpoint, the 'Tunnel' is decapsulated, and the 'Payload' is retrieved.</p> <p>Figure 5: Tunneling</p> <p>VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.</p>
name; receiving a secure domain	<p>VPN Overview, Page 26: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpax.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses.</p> <p>RFC 1035, Page 4:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. RFC 1035, Page 4:</p> 
<p>receiving from the secure domain name service a response message containing the secure computer network</p>	<p>RFC 1035, Page 4:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
address corresponding to the secure domain name; and	
sending an access request message to the secure computer network address using a virtual private network communication link.	<p>VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet).</p> <p>VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.</p> <p>VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.</p>  <p><i>Figure 3: Using a VPN to connect two remote sites</i></p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p>VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork.</p> <p>VPN Overview, Page 10:</p> <div data-bbox="662 898 1307 1207" data-label="Diagram"> <p>The diagram illustrates the tunneling process. On the left, a 'Payload' is shown as a small rectangular block. This payload is combined with a 'Transit Internet Header' to form a 'Tunneled Payload', represented as a larger rectangular block with an arrow pointing to the right. This tunneled payload is sent through a 'Transit Internetwork', which is depicted as a cloud. The path through the cloud is labeled as a 'Tunnel'. On the right side of the cloud, the tunneled payload is received and the original 'Payload' is extracted. 'Tunnel Endpoints' are indicated by lines pointing to the source and destination nodes of the tunnel.</p> </div> <p><i>Figure 5: Tunneling</i></p> <p>VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.</p> <p>VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p>VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	<p>access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation.</p> <p>VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p>VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with an ISP to deploy a nationwide set of FEPs. These <u>FEPs can establish tunnels across the Internet</u> to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network.</p> <p>VPN Overview, Page 22:</p> <div data-bbox="662 961 1266 1155" data-label="Diagram"> <p>The diagram illustrates the compulsory tunneling process. On the left, a 'Dial-Up Client' (represented by a computer monitor and keyboard) is connected via a 'PPP Connection' to an 'ISP FEP' (Internet Service Provider Front-End Processor), depicted as a server rack. From the ISP FEP, traffic is sent through the 'Internet' (represented by a cloud) to a 'Tunnel' (represented by a shaded bar) and finally to a 'Tunnel Server' (another server rack) located on an 'intranet'.</p> </div> <p>Figure 9: Compulsory tunneling</p> <p>VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p>VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication--despite the fact that this communication occurs over a public internetwork.</p>
35. The apparatus of claim 33, wherein	VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
<p>the response message contains provisioning information for the virtual private network.</p>	<p>network between the branch office router and the corporate hub router across the Internet.</p>  <p><i>Figure 3: Using a VPN to connect two remote sites</i></p> <p>VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.</p> <p>User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.</p> <p>VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel.</p> <p>VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.</p> <p>VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design.</p> <p>VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network</p>

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	communication-despite the fact that this communication occurs over a public internetwork.

Appendix C
Citations to Exemplary Description in the Kosiur Reference*

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called <i>tunneling</i>.</p> <p>Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual <i>pipe</i>. This pipe makes the routed network totally transparent to users.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p> <div data-bbox="568 987 1266 1260" data-label="Diagram"> <p>The diagram illustrates a network tunnel. On the left, 'Workstation A' is connected to 'Security gateway 1'. A dashed line representing a tunnel goes through a cloud labeled 'Internet'. On the right, 'Security gateway 2' is connected to 'Server B'. Below the tunnel, a data packet is shown with 'Source' and 'Destination' fields. An arrow labeled 'Encrypted' points to a box containing '1 2 A B data', representing the data being transmitted through the tunnel.</p> </div> <p style="text-align: center;">FIGURE 3.2 Schematic of a tunnel.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
<p>receiving a secure domain name;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p>

* - The cited passages are an indication of where in the Kosiur reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link,</p>

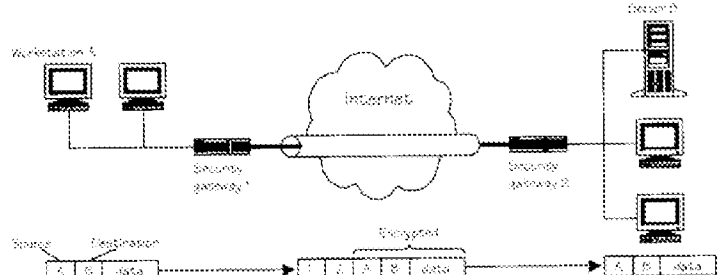
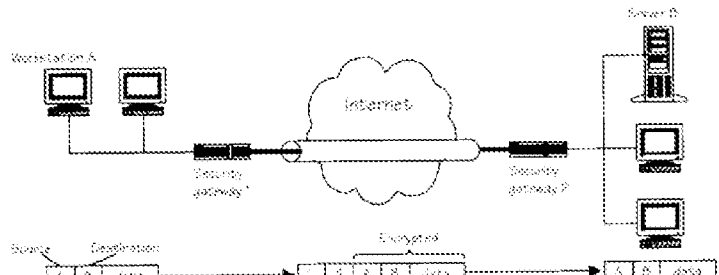
7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p>
<p>4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. When the connection is no longer needed, it's torn down, making the bandwidth and other network resources available for other uses.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p> <p>Page 132: (4) Via RADIUS, the proxy server instructs the remote access server to grant (or deny) the user access.</p> <p>The remote access server will open the tunneled connection, creating a tunnel if necessary.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p> <p>Pages 308 - 311: But, if traffic prioritization using classes is insufficient for your needs, and you choose to allocate network resources between real-time and non-real-time applications, then you have two choices. Either you can statically allocate the resources or you can allow resources to be reserved dynamically.</p> <p><i>Static resource allocation</i> enables you to reserve a portion of a network's capacity for a particular type of traffic, usually based on protocol, application, or user. In many enterprise networks, routers are often</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>configured to devote a certain amount of their capacity to SNA traffic, for instance, to accommodate the requirements of legacy data transactions.</p> <p>.....</p> <p>When the capacity is reserved for a specific protocol or application, the capacity should be large enough to meet the demands of all traffic of that type. If not, the traffic exceeding the allotted capacity will most likely be subject to delays and/or discards. If the allotted capacity isn't used, it's possible for other traffic to use the remaining bandwidth.</p> <p>.....</p> <p>RSVP operates on top of IP; it is an Internet control protocol like IGMP or ICMP, but it is not a routing protocol. It uses underlying routing protocols to determine the destination for reservation requests. As routing paths change, RSVP adapts its reservation to new paths if reservations are in place. The RSVP protocol is used by routers to deliver QoS control requests to all nodes along the paths of the flows (see Figure 15.3) and to establish and maintain state to provide the requested service. After a reservation has been made, routers supporting RSVP determine the route and the QoS class for each incoming packet and the scheduler makes forwarding decisions for every outgoing packet.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
<p>10. The method according to claim 1, wherein the virtual private network includes the Internet.</p>	<p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called <i>tunneling</i>.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
<p>12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Page 40: Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual <i>pipe</i>. This pipe makes the routed network totally transparent to users.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p> <p>Page 133: Upon authorization, the PPTP server will accept tunneled packets from the remote user and forward the packets to the appropriate destination on the corporate network.</p> <p>Pages 276 - 277: Before a secure tunnel can be established between two security gateways, or between a remote host and a gateway, these devices have to be authenticated by each other and agree on a key.</p>

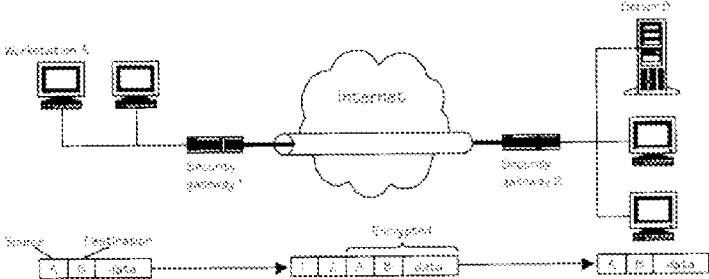
7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>.....</p> <p>If a security gateway isn't shipped with hard-wired keys, the gateway would be set to randomly generate its own key pair. A digital certificate then would be signed with the private key and sent to the appropriate certificate authority, either an in-house certificate server or a third-party CA like VeriSign. When the certificate is approved, that certificate is available from the CA for use by other security gateways and remote clients to authenticate the site before any data is exchanged (see Figure 13.2).</p>
<p>13. The method of claim 1, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p>
<p>14. The method of claim 1, performed by a software module.</p>	<p>See claim 1, which is performed by software at the client computer (i.e., the VPN client).</p> <p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Pages 41-42:</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	 <p style="text-align: center;">FIGURE 3.2 Schematic of a tunnel.</p> <p>Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary.</p>
<p>15. The method of claim 1, performed by a client computer.</p>	<p>See claim 1, which is performed by software at the client computer (i.e., the VPN client).</p> <p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Pages 41-42:</p>  <p style="text-align: center;">FIGURE 3.2 Schematic of a tunnel.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
<p>17. A computer-readable storage medium, comprising:</p>	<p>Page 111: On the other hand, if you have mobile workers and small branch offices that will need to dial into the corporate net via an ISP, then IPSec client software has to be installed on the appropriate computers--laptops for the mobile workers, perhaps the branch office's desktop computers.</p> <p>Page 162: If you want end-to-end encryption, for instance, you would install IPSec-compliant clients on your mobile workers' computers and expect the ISP to handle encrypted packets from clients all the way to your network server.</p>
<p>a storage area; and</p>	<p>Page 111: On the other hand, if you have mobile workers and small branch offices that will need to dial into the corporate net via an ISP, then IPSec client software has to be installed on the appropriate computers--laptops for the mobile workers, perhaps the branch office's desktop computers.</p> <p>Page 162: If you want end-to-end encryption, for instance, you would install IPSec-compliant clients on your mobile workers' computers and expect the ISP to handle encrypted packets from clients all the way to your network server.</p>
<p>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called <i>tunneling</i>.</p> <p>Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual <i>pipe</i>. This pipe makes the routed network totally transparent to users.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	 <p style="text-align: center;">FIGURE 3.2 Schematic of a tunnel.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
<p>name;</p> <p>receiving a secure domain</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p>

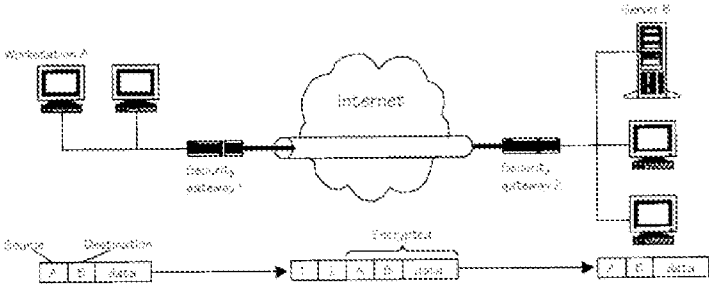
7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p>
<p>20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. When the connection is no longer needed, it's torn down, making the bandwidth and other network resources available for other uses.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p> <p>Page 132: (4) Via RADIUS, the proxy server instructs the remote access server to grant (or deny) the user access.</p> <p>The remote access server will open the tunneled connection, creating a tunnel if necessary.</p>

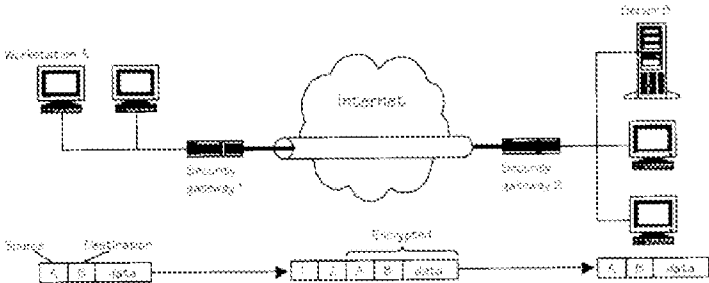
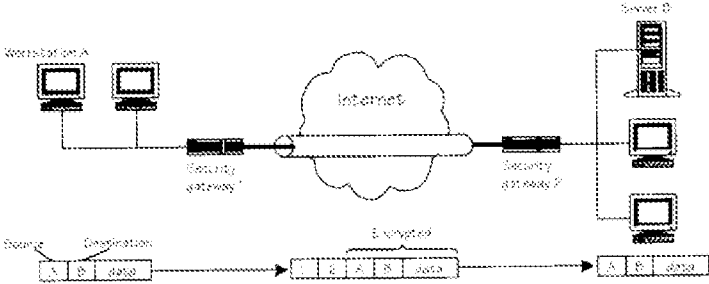
7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p> <p>Pages 308 - 311: But, if traffic prioritization using classes is insufficient for your needs, and you choose to allocate network resources between real-time and non-real-time applications, then you have two choices. Either you can statically allocate the resources or you can allow resources to be reserved dynamically.</p> <p><i>Static resource allocation</i> enables you to reserve a portion of a network's capacity for a particular type of traffic, usually based on protocol, application, or user. In many enterprise networks, routers are often configured to devote a certain amount of their capacity to SNA traffic, for instance, to accommodate the requirements of legacy data transactions.</p> <p>.....</p> <p>When the capacity is reserved for a specific protocol or application, the capacity should be large enough to meet the demands of all traffic of that type. If not, the traffic exceeding the allotted capacity will most likely be subject to delays and/or discards. If the allotted capacity isn't used, it's possible for other traffic to use the remaining bandwidth.</p> <p>.....</p> <p>RSVP operates on top of IP; it is an Internet control protocol like IGMP or ICMP, but it is not a routing protocol. It uses underlying routing protocols to determine the destination for reservation requests. As routing paths change, RSVP adapts its reservation to new paths if reservations are in place. The RSVP protocol is used by routers to deliver QoS control requests to all nodes along the paths of the flows (see Figure 15.3) and to establish and maintain state to provide the requested service. After a reservation has been made, routers supporting RSVP determine the route and the QoS class for each incoming packet and the scheduler makes forwarding decisions for every outgoing packet.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	<p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called <i>tunneling</i>.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	<p>Page 40: Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual <i>pipe</i>. This pipe makes the routed network totally transparent to users.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p> <p>Page 133: Upon authorization, the PPTP server will accept tunneled packets from the remote user and forward the packets to the appropriate destination on the corporate network.</p> <p>Pages 276 - 277: Before a secure tunnel can be established between two security gateways, or between a remote host and a gateway, these devices have to be authenticated by each other and agree on a key.</p> <p>. . . .</p> <p>If a security gateway isn't shipped with hard-wired keys, the gateway would be set to randomly generate its own key pair. A digital certificate then would be signed with the private key and sent to the appropriate certificate authority, either an in-house certificate server or a third-party CA like VeriSign. When the certificate is approved, that certificate is available from the CA for use by other security gateways and remote clients to authenticate the site before any data is exchanged (see Figure 13.2).</p>
29. The computer-readable medium according to claim 17,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service (DNS)</i> for resolving device names and IP addresses. This makes both

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>wherein sending the access request message comprises sending the access request</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
message at the client computer.	<p>permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p>
<p>30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.</p>	<p>See claim 1, which is performed by software at the client computer (i.e., the VPN client).</p> <p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Pages 41-42:</p>  <p>FIGURE 3.2 Schematic of a tunnel.</p> <p>Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary.</p>
<p>31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.</p>	<p>See claim 1, which is performed by software at the client computer (i.e., the VPN client).</p> <p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Pages 41-42:</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	 <p data-bbox="773 907 1084 932">FIGURE 3.2 Schematic of a tunnel.</p> <p data-bbox="553 940 1438 989">Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary.</p> <p data-bbox="553 989 1438 1037">Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
<p data-bbox="142 1062 457 1113">33. A data processing apparatus, comprising:</p>	<p data-bbox="553 1062 630 1087">Page 41:</p>  <p data-bbox="773 1390 1084 1415">FIGURE 3.2 Schematic of a tunnel.</p>
<p data-bbox="220 1449 357 1474">a processor, and</p>	<p data-bbox="553 1449 1438 1497">Page 34: Another factor of great importance to network managers is the reliability of the product or service. For VPNs, reliability concerns focus on two different components—the hardware (and associated software)</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
<p>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>and the communications services (i.e., the Internet). Using standard components in the hardware-microprocessors, proven interface cards, and so on-is important, as is the maintainability of the hardware.</p> <p>Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers.</p> <p>Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called <i>tunneling</i>.</p> <p>Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual <i>pipe</i>. This pipe makes the routed network totally transparent to users.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p> <div data-bbox="574 953 1279 1234" data-label="Diagram"> <p>The diagram illustrates a secure communication path. On the left, 'Workstation A' is connected to 'Secure gateway 1'. A line representing a tunnel connects 'Secure gateway 1' to 'Secure gateway 2', passing through a cloud labeled 'Internet'. 'Secure gateway 2' is connected to 'Workstation B'. Below this, a data flow is shown: 'Source' sends 'A B data' through a 'Tunnel' (represented by a dashed box) to 'Destination', which receives 'A B data'. The data within the tunnel is labeled 'Encrypted'.</p> </div> <p>FIGURE 3.2 Schematic of a tunnel.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>
<p>receiving a secure domain name;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DNS server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified <i>Domain Name Service</i> (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage.</p> <p>Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.</p> <p>Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link,</p>

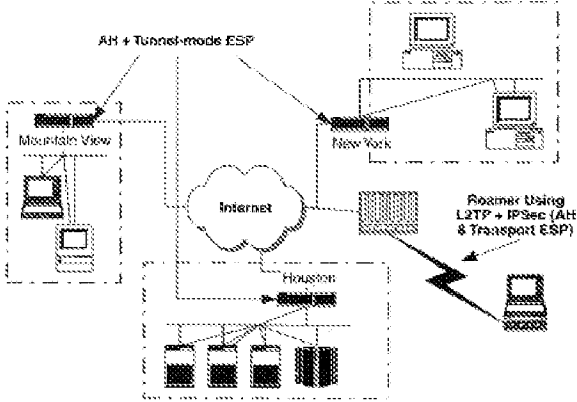
7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p>
<p>35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. When the connection is no longer needed, it's torn down, making the bandwidth and other network resources available for other uses.</p> <p>Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, <i>private</i> has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.</p> <p>Page 132: (4) Via RADIUS, the proxy server instructs the remote access server to grant (or deny) the user access.</p> <p>The remote access server will open the tunneled connection, creating a tunnel if necessary.</p> <p>Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and your corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.</p> <p>The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find.</p> <p>The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall.</p> <p>If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.</p> <p>Pages 308 - 311: But, if traffic prioritization using classes is insufficient for your needs, and you choose to allocate network resources between real-time and non-real-time applications, then you have two choices. Either you can statically allocate the resources or you can allow resources to be reserved dynamically.</p> <p><i>Static resource allocation</i> enables you to reserve a portion of a network's capacity for a particular type of traffic, usually based on protocol, application, or user. In many enterprise networks, routers are often</p>

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	<p>configured to devote a certain amount of their capacity to SNA traffic, for instance, to accommodate the requirements of legacy data transactions.</p> <p>.....</p> <p>When the capacity is reserved for a specific protocol or application, the capacity should be large enough to meet the demands of all traffic of that type. If not, the traffic exceeding the allotted capacity will most likely be subject to delays and/or discards. If the allotted capacity isn't used, it's possible for other traffic to use the remaining bandwidth.</p> <p>.....</p> <p>RSVP operates on top of IP; it is an Internet control protocol like IGMP or ICMP, but it is not a routing protocol. It uses underlying routing protocols to determine the destination for reservation requests. As routing paths change, RSVP adapts its reservation to new paths if reservations are in place. The RSVP protocol is used by routers to deliver QoS control requests to all nodes along the paths of the flows (see Figure 15.3) and to establish and maintain state to provide the requested service. After a reservation has been made, routers supporting RSVP determine the route and the QoS class for each incoming packet and the scheduler makes forwarding decisions for every outgoing packet.</p> <p>Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.</p>

Appendix D
Citations to Exemplary Description in the Kaufman Reference*

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis.</p> <p>Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location.</p> <p>Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection.</p> <p>....</p> <p>An extranet is an instance of a virtual private network (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy.</p> <p>Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>

* - The cited passages are an indication of where in the Kaufman reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 <p data-bbox="586 1052 737 1066">Figure 9.1 IPsec VPN</p> <p data-bbox="553 1079 1455 1266">Page 200: The simplest form of management is manual management, in which a person manually configures each system with keying material and security association management data relevant to secure communication with other systems. Manual techniques are practical in small, static environments but they do not scale well. For example, a company could create a Virtual Private Network (VPN) using IPsec in security gateways at several sites. If the number of sites is small, and since all the sites come under the purview of a single administrative domain, this is likely to be a feasible context for manual management techniques. In this case, the security gateway might selectively protect traffic to and from other sites within the organization using a manually configured key, while not protecting traffic for other destinations.</p>
receiving a secure domain name;	<p data-bbox="553 1272 1455 1383">Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p data-bbox="553 1388 1455 1501">Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.</p>
<p>10. The method according to claim 1, wherein the virtual private network includes the Internet.</p>	<p>Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs.</p> <p>Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another.</p> <p>Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy--in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets--which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.</p>
<p>12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as</p>

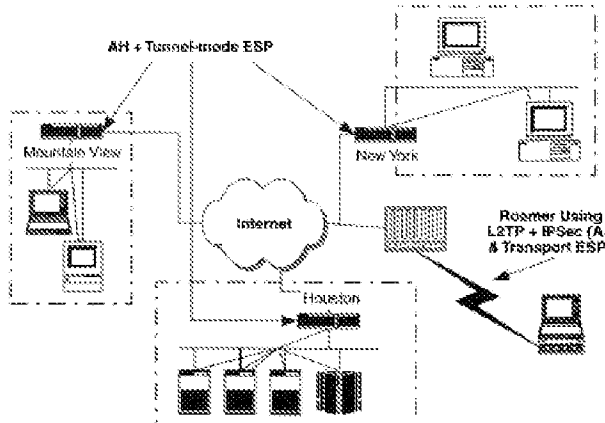
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>13. The method of claim 1, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein sending the query message comprises sending the query message at the</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
client computer;	<p>dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
wherein receiving the response message comprises receiving the response message at the client computer,	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., <u>mozart@foo.bar.com</u></p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>14. The method of claim 1, performed by a software module.</p>	<p>Page 133: Many network devices use <i>Trivial File Transfer Protocol</i> (TFTP) to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics.</p> <p>Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways.</p> <p>Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):</p>
<p>15. The method of claim 1, performed by a client computer.</p>	<p>Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p>
<p>17. A computer-readable storage medium, comprising:</p>	<p>Page 215: The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling. The per-packet computational costs will be manifested by increased latency and, possibly, reduced throughput. Use of SA/key management protocols, especially ones that employ public key cryptography, also adds computational performance costs to use of IPsec. These per association computational costs will be manifested in terms of increased latency in association establishment. For many hosts, it is anticipated that software-based cryptography will not appreciably reduce throughput, but hardware may be required for security gateways (since they represent aggregation points), and for some hosts.</p>
<p>a storage area; and</p>	<p>Page 215: The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling.</p>
<p>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis.</p> <p>Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location.</p> <p>Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.)</p> <p>Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations.</p> <p>Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.</p> <p>Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection.</p> <p>....</p> <p>An extranet is an instance of a <i>virtual private network</i> (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy.</p> <p>Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 <p data-bbox="584 1071 747 1092">Figure 9.1 IPsec VPN.</p>
<p data-bbox="136 1176 194 1197">name;</p> <p data-bbox="292 1155 503 1176">receiving a secure domain</p>	<p data-bbox="542 1155 1445 1270">Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p data-bbox="542 1270 1445 1386">Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as <i>www.wiley.com</i>) and IP network addresses (such as <i>10.235.134.17</i>). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p data-bbox="542 1386 1445 1501">Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>receiving from the domain</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
<p>name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p style="padding-left: 20px;">a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote</p>

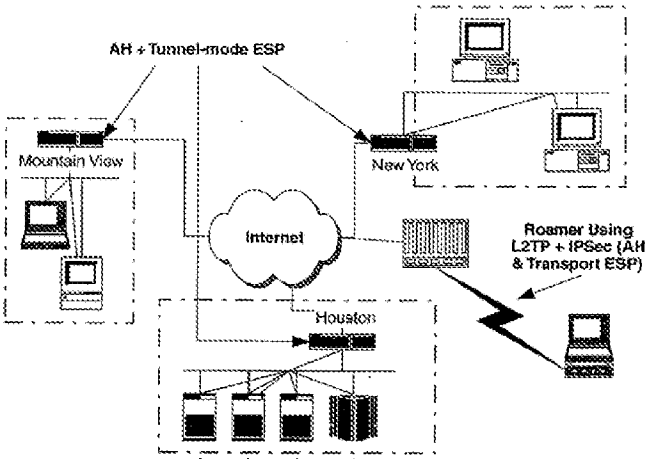
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	host can receive an IP address internal to its home network.
<p>20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.</p>
<p>26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.</p>	<p>Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs.</p> <p>Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another.</p> <p>Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy--in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets--which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.</p>
<p>28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
29. The computer-readable medium according to claim 17,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
wherein sending the query message comprises sending the query message at the client computer;	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses</p>

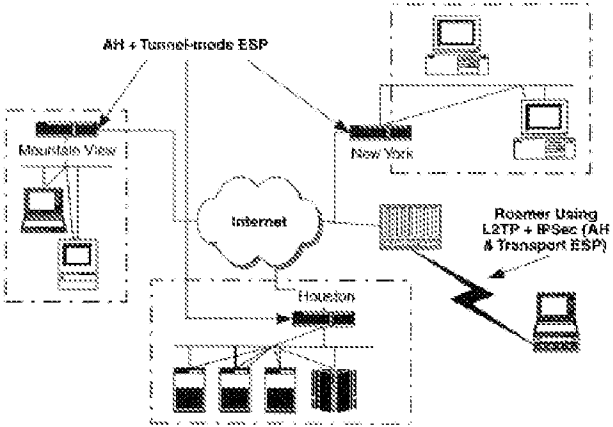
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>(such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.</p>	<p>Page 133: Many network devices use <i>Trivial File Transfer Protocol</i> (TFTP) to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics.</p> <p>Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways.</p> <p>Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):</p>
<p>31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.</p>	<p>Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p>
<p>33. A data processing apparatus, comprising:</p>	<p>Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 <p data-bbox="589 1098 760 1119">Figure 3.1 IPsec VPN.</p>
<p data-bbox="224 1157 354 1178">a processor, and</p>	<p data-bbox="553 1157 1453 1251">Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations.</p> <p data-bbox="553 1255 1422 1339">Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.</p>
<p data-bbox="144 1346 529 1486">memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p data-bbox="553 1346 1453 1461">Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis.</p> <p data-bbox="553 1465 1453 1486">Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location.</p> <p>Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.)</p> <p>Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations.</p> <p>Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.</p> <p>Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection.</p> <p>....</p> <p>An extranet is an instance of a <i>virtual private network (VPN)</i>, described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy.</p> <p>Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 <p data-bbox="589 1077 748 1094">Figure 9.1 IPsec VPN.</p>
<p data-bbox="144 1203 196 1224">name;</p> <p data-bbox="293 1182 509 1203">receiving a secure domain</p>	<p data-bbox="553 1182 1455 1297">Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p data-bbox="553 1299 1455 1415">Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p data-bbox="553 1417 1455 1507">Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	<p>RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>

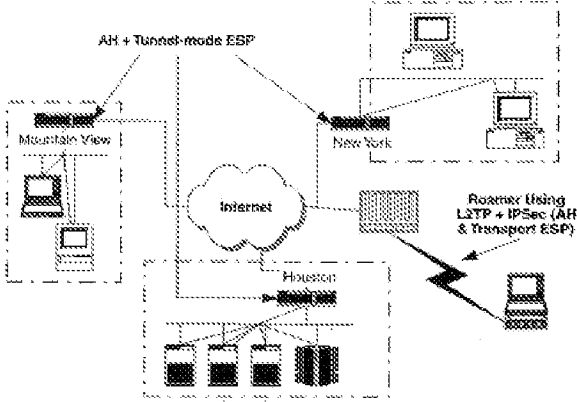
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network</p>

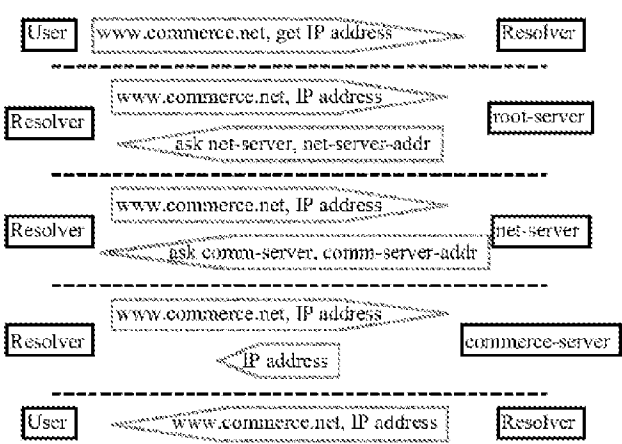
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.

Appendix E
Citations to Exemplary Description in the Kaufman and Galvin References*

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>Kaufman, Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis.</p> <p>Kaufman, Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location.</p> <p>Kaufman, Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection.</p> <p>....</p> <p>An extranet is an instance of a virtual private network (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy.</p> <p>Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>

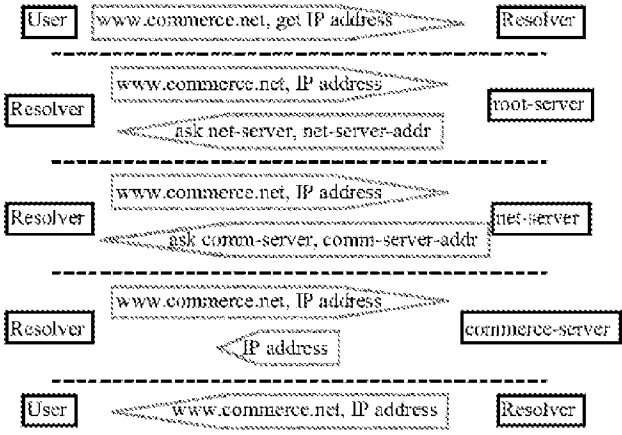
* - The cited passages are an indication of where in the Kaufman and Galvin references, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	 <p data-bbox="586 1052 737 1066">Figure 9.1 IPsec VPN.</p> <p data-bbox="553 1079 1451 1266">Kaufman, Page 200: The simplest form of management is manual management, in which a person manually configures each system with keying material and security association management data relevant to secure communication with other systems. Manual techniques are practical in small, static environments but they do not scale well. For example, a company could create a Virtual Private Network (VPN) using IPsec in security gateways at several sites. If the number of sites is small, and since all the sites come under the purview of a single administrative domain, this is likely to be a feasible context for manual management techniques. In this case, the security gateway might selectively protect traffic to and from other sites within the organization using a manually configured key, while not protecting traffic for other destinations.</p>
receiving a secure domain name;	<p data-bbox="553 1272 1435 1381">Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p data-bbox="553 1388 1435 1499">Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p>

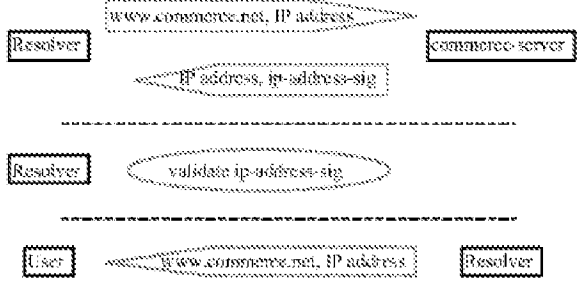
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Galvin § 2.2:</p>  <p>The diagram illustrates the hierarchical resolution of a domain name to an IP address. It shows a sequence of queries and responses between a User, a Resolver, and various DNS servers (root-server, net-server, commerce-server). The User sends a query for 'www.commerce.net, get IP address' to the Resolver. The Resolver then queries the root-server for 'www.commerce.net, IP address'. The root-server responds with 'ask net-server, net-server-addr'. The Resolver then queries the net-server for 'www.commerce.net, IP address'. The net-server responds with 'ask comm-server, comm-server-addr'. The Resolver then queries the commerce-server for 'www.commerce.net, IP address'. The commerce-server responds with 'IP address'. Finally, the Resolver sends the 'www.commerce.net, IP address' back to the User.</p> <p>Galvin § 3: 3. Secure Domain Name System Security enhancements for the DNS [9] have been drafted</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records managed by the DNS.</p> <p>Galvin § 3.1.3: Secure DNS Server Operation The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned.</p> <p>Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address.</p> <p>Galvin § 3.2:</p> <pre> sequenceDiagram participant User participant Resolver participant RootServer as Root Server participant NetServer as Net Server participant Resolver2 as Resolver User->>Resolver: {www.commerce.net, get IP address} Resolver->>RootServer: {www.commerce.net, IP address} RootServer-->>Resolver: {ask net-server, net-server-addr, net-domain-pk, net-domain-sig} Resolver->>Resolver: validate net-domain-pk Resolver->>NetServer: {net, IP address} NetServer-->>Resolver: {IP address, SIG} Resolver->>Resolver: validate IP address </pre>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>The diagram illustrates three distinct DNS resolution processes:</p> <ul style="list-style-type: none"> Scenario 1: A Resolver sends a query for "www.commerce.net, IP address" to a "dns-server". The server returns a response containing "193.commerce-server, commerce-server-addr, commerce-domain-pk, commerce-domain-sig". The Resolver then sends a validation request "validate commerce-domain-pk". Scenario 2: A Resolver sends a query for "commerce.net, IP address" to a "commerce-server". The server returns a response containing "IP address, SIG". The Resolver then sends a validation request "validate IP address". Scenario 3: A Resolver sends a query for "www.commerce.net, IP address" to an "authenticated-server". The server returns a response containing "IP address, ip-address-sig". The Resolver then sends a validation request "validate ip-address-sig". Scenario 4: A "User" sends a query for "www.commerce.net, IP address" to a "Resolver".
<p>receiving from the secure domain name service a response message containing the secure computer network address</p>	<p>Galvin § 2.2:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>corresponding to the secure domain name; and</p>	 <pre> sequenceDiagram participant User participant Resolver participant RootServer as root-server participant NetServer as net-server participant CommerceServer as commerce-server User->>Resolver: www.commerce.net, get IP address Resolver->>RootServer: www.commerce.net, IP address RootServer-->>Resolver: ask net-server, net-server-addr Resolver->>NetServer: www.commerce.net, IP address NetServer-->>Resolver: ask comm-server, commi-server-addr Resolver->>CommerceServer: www.commerce.net, IP address CommerceServer-->>Resolver: IP address Resolver-->>User: www.commerce.net, IP address </pre> <p>Galvin § 3: 3. Secure Domain Name System Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS.</p> <p>Galvin § 3.1.3: Secure DNS Server Operation The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned.</p> <p>Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address.</p> <p>Galvin § 3.2:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>The diagram illustrates a sequence of steps in a prior art reference, showing interactions between a User, Resolver, and various servers (net-server, COMMERCE-SERVER). The steps are separated by dashed lines and include actions like sending requests, receiving responses, and performing validation tasks.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	 <pre> sequenceDiagram participant Resolver1 as Resolver participant CommerceServer as commerce server Resolver1->>CommerceServer: www.commerce.net, IP address CommerceServer-->>Resolver1: IP address, ip-address-sig Resolver1->>User: validate ip-address-sig participant User User->>Resolver2 as Resolver: www.commerce.net, IP address </pre>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Kaufman, Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.
10. The method according to claim 1, wherein the virtual private network includes the Internet.	<p>Kaufman, Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs.</p> <p>Kaufman, Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another.</p> <p>Kaufman, Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy--in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets--which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.</p>
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	<p>Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
13. The method of claim 1, wherein receiving the secure domain	Kaufman, Page 125: The technologies described in the following sections are among those vital to network

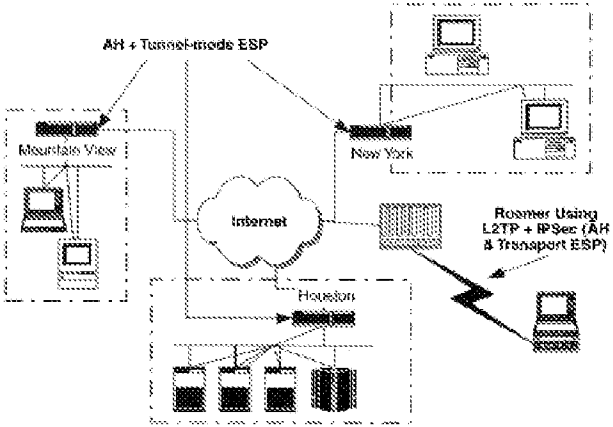
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>name comprises receiving the secure domain name at a client computer from a user;</p>	<p>operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., <u>mozart@foo.bar.com</u></p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working</p>

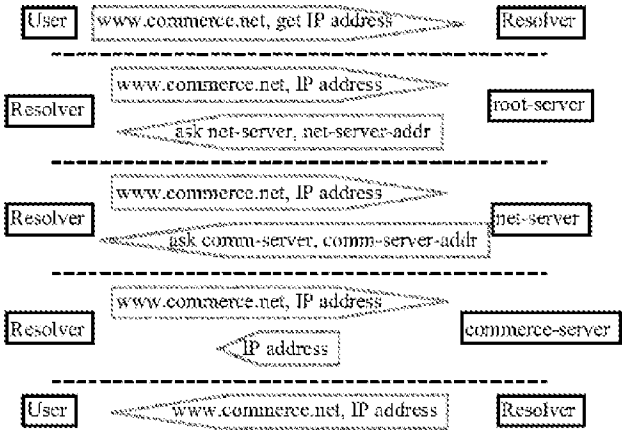
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host</p>

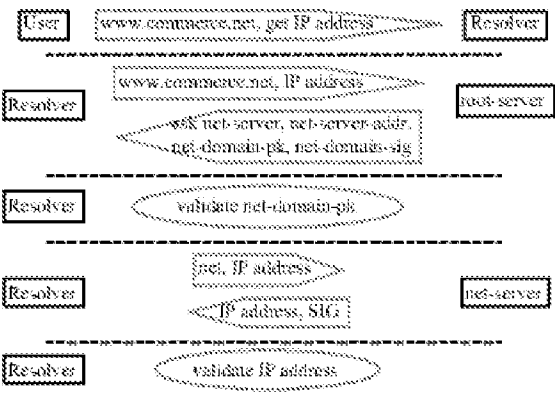
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>names to IP addresses (and vice versa) in the Internet.</p> <p>Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>14. The method of claim 1, performed by a software module.</p>	<p>Kaufman, Page 133: Many network devices use <i>Trivial File Transfer Protocol (TFTP)</i> to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics.</p> <p>Kaufman, Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways.</p> <p>Kaufman, Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):</p>
<p>15. The method of claim 1, performed by a client computer.</p>	<p>Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.
17. A computer-readable storage medium, comprising:	Kaufman, Page 215: The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling. The per-packet computational costs will be manifested by increased latency and, possibly, reduced throughput. Use of SA/key management protocols, especially ones that employ public key cryptography, also adds computational performance costs to use of IPsec. These per association computational costs will be manifested in terms of increased latency in association establishment. For many hosts, it is anticipated that software-based cryptography will not appreciably reduce throughput, but hardware may be required for security gateways (since they represent aggregation points), and for some hosts.
a storage area; and	Kaufman, Page 215: The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling.
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Kaufman, Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis. Kaufman, Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location. Kaufman, Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly

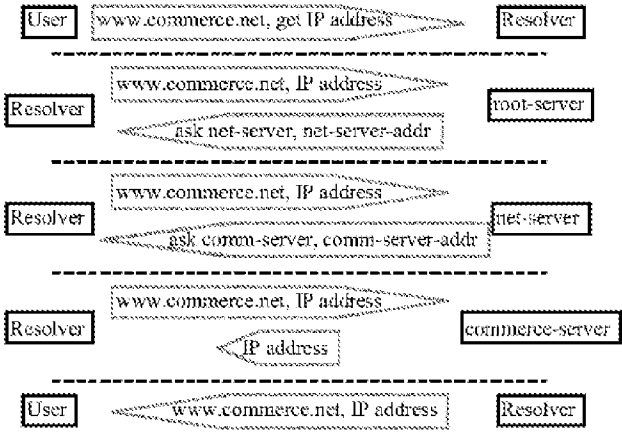
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.)</p> <p>Kaufman, Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations.</p> <p>Kaufman, Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.</p> <p>Kaufman, Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection.</p> <p>....</p> <p>An extranet is an instance of a <i>virtual private network (VPN)</i>, described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy.</p> <p>Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	 <p data-bbox="589 1077 748 1094">Figure 8.1 IPsec VPN.</p>
<p data-bbox="136 1178 201 1203">name;</p> <p data-bbox="293 1157 513 1182">receiving a secure domain</p>	<p data-bbox="553 1157 1438 1272">Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p data-bbox="553 1276 1438 1392">Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p data-bbox="553 1396 1438 1505">Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., <u>mozart@foo.bar.com</u></p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Galvin § 2.2:</p>  <p>The diagram illustrates the iterative DNS resolution process for the domain <code>www.commerce.net</code>. It shows a sequence of queries and responses between a User and various Resolver servers:</p> <ul style="list-style-type: none"> Step 1: The User sends a query <code>www.commerce.net, get IP address</code> to a Resolver. Step 2: The Resolver sends a query <code>www.commerce.net, IP address</code> to a root-server. Step 3: The root-server responds with <code>ask net-server, net-server-addr</code>. Step 4: The Resolver sends a query <code>www.commerce.net, IP address</code> to a net-server. Step 5: The net-server responds with <code>ask comm-server, comm-server-addr</code>. Step 6: The Resolver sends a query <code>www.commerce.net, IP address</code> to a commerce-server. Step 7: The commerce-server responds with the final <code>IP address</code>. Step 8: The Resolver sends the final response <code>www.commerce.net, IP address</code> back to the User. <p>Galvin § 3: 3. Secure Domain Name System Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records managed by the DNS.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>Galvin § 3.1.3: Secure DNS Server Operation The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned.</p> <p>Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address.</p> <p>Galvin § 3.2:</p>  <pre> sequenceDiagram participant User participant Resolver User->>Resolver: www.commerce.net, get IP address Resolver->>RootServer: www.commerce.net, IP address RootServer-->>Resolver: www.net-server, net-server-addr, net-domain-pk, net-domain-sig Resolver->>Resolver: validate net-domain-pk Resolver->>NetServer: [net, IP address] NetServer-->>Resolver: IP address, SIG Resolver->>Resolver: validate IP address </pre> <p>...</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>The diagram illustrates three distinct DNS resolution processes:</p> <ul style="list-style-type: none"> Scenario 1: A Resolver sends a query for 'www.commerce.net, IP address' to a 'dns-server'. The server returns a response containing '193.commerce-server, commerce-server-addr, commerce-domain-pk, commerce-domain-sig'. The Resolver then performs a 'validate commerce-domain-pk' step. Scenario 2: A Resolver sends a query for 'commerce.net, IP address' to a 'commerce-server'. The server returns a response containing 'IP address, SIG'. The Resolver then performs a 'validate IP address' step. Scenario 3: A Resolver sends a query for 'www.commerce.net, IP address' to an 'authenticated-server'. The server returns a response containing 'IP address, ip-address-sig'. The Resolver then performs a 'validate ip-address-sig' step. Scenario 4: A User sends a query for 'www.commerce.net, IP address' to a Resolver.
<p>receiving from the domain name service a response message containing the secure computer network address</p>	<p>Galvin § 2.2:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>corresponding to the secure domain name; and</p>	 <pre> sequenceDiagram participant User participant Resolver participant root-server participant net-server participant commerce-server User->>Resolver: www.commerce.net, get IP address Resolver->>root-server: www.commerce.net, IP address root-server-->>Resolver: ask net-server, net-server-addr Resolver->>net-server: www.commerce.net, IP address net-server-->>Resolver: ask comm-server, commi-server-addr Resolver->>commerce-server: www.commerce.net, IP address commerce-server-->>Resolver: IP address Resolver-->>User: www.commerce.net, IP address </pre> <p>Galvin § 3: 3. Secure Domain Name System Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS.</p> <p>Galvin § 3.1.3: Secure DNS Server Operation The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned.</p> <p>Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address.</p> <p>Galvin § 3.2:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>The diagram illustrates a sequence of steps in a prior art reference, showing interactions between a User, Resolver, and net-server. The steps are as follows:</p> <ol style="list-style-type: none"> User sends "www.commerce.net, get IP address" to Resolver. Resolver sends "www.commerce.net, IP address" to net-server. net-server sends "ask net-server, net-server-addr, net-domain-pk, net-domain-sig" to Resolver. Resolver sends "validate net-domain-pk" to net-server. net-server sends "net, IP address" to Resolver. Resolver sends "IP address, SIG" to net-server. net-server sends "validate IP address" to Resolver. Resolver sends "www.commerce.net, IP address" to net-server. net-server sends "ask commerce-server, commerce-server-addr, commerce-domain-pk, commerce-domain-sig" to Resolver. Resolver sends "validate commerce-domain-pk" to net-server. net-server sends "commerce.net, IP address" to Resolver. Resolver sends "IP address, SIG" to net-server. net-server sends "validate IP address" to Resolver.

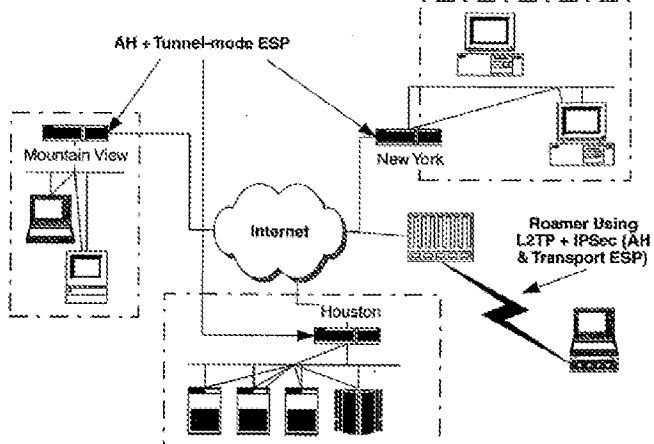
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<pre> sequenceDiagram participant Resolver participant CommerceServer as commerce server Resolver->>CommerceServer: www.commerce.net, IP address CommerceServer-->>Resolver: IP address, ip-address-sig Resolver->>User: validate ip-address-sig User->>Resolver: www.commerce.net, IP address </pre>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Kaufman, Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	<p>Kaufman, Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs.</p> <p>Kaufman, Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another.</p> <p>Kaufman, Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy--in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets--which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.</p>
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	<p>Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
29. The computer-readable medium according to claim 17,	

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p> <p>Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p> <p>Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
<p>30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.</p>	<p>Kaufman, Page 133: Many network devices use <i>Trivial File Transfer Protocol</i> (TFTP) to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics.</p> <p>Kaufman, Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways.</p> <p>Kaufman, Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):</p>
<p>31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.</p>	<p>Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p>
<p>33. A data processing apparatus, comprising:</p>	<p>Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p>  <p>Figure 2.1 IPsec VPN.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>a processor, and</p>	<p>Kaufman, Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations.</p> <p>Kaufman, Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.</p>
<p>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>Kaufman, Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis.</p> <p>Kaufman, Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location.</p> <p>Kaufman, Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.)</p> <p>Kaufman, Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations.</p> <p>Kaufman, Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.</p> <p>Kaufman, Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection.</p>

7,188,180 Claim Elements

Description for Claimed Elements in the Kaufman and Galvin Prior Art References

An extranet is an instance of a *virtual private network (VPN)*, described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy.

Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.

End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.

A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.

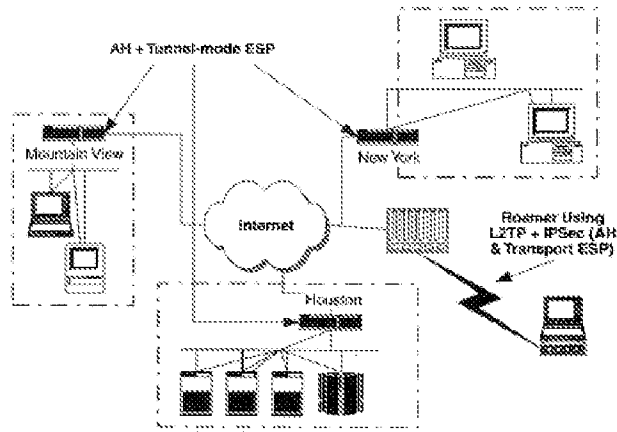
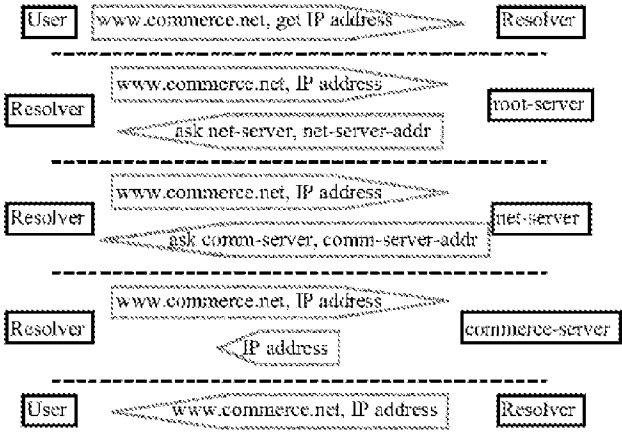


Figure 9.1 IPsec VPN.

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>receiving a secure domain name;</p>	<p>Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel.</p> <p>Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of <i>name-to-address</i> and <i>address-to-name</i> mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or <i>resolve</i>) a name to an address (or vice versa) and a server-to-server update mechanism called a <i>zone transfer</i>.</p> <p>Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF <i>DNS Security</i> (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).</p> <p>Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the <i>secure</i> IP address) in one that is routable from the given location.</p> <p>Kaufman, Page 191: 1. User ID</p> <p>a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com</p> <p>Kaufman, Page 243: <i>Domain Name Service</i>. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Galvin § 2.2:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	 <pre> sequenceDiagram participant User participant Resolver participant RootServer as root-server participant NetServer as net-server participant CommerceServer as commerce-server User->>Resolver: www.commerce.net, get IP address Resolver->>RootServer: www.commerce.net, IP address RootServer-->>Resolver: ask net-server, net-server-addr Resolver->>NetServer: www.commerce.net, IP address NetServer-->>Resolver: ask comm-server, commi-server-addr Resolver->>CommerceServer: www.commerce.net, IP address CommerceServer-->>Resolver: IP address Resolver-->>User: www.commerce.net, IP address </pre> <p>Galvin § 3: 3. Secure Domain Name System Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS.</p> <p>Galvin § 3.1.3: Secure DNS Server Operation The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned.</p> <p>Galvin § 3.2: [S]uppose a user application needs the IP address of the host <u>www.commerce.net</u>. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address.</p> <p>Galvin § 3.2:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>The diagram illustrates a multi-step DNS resolution process. It begins with a User requesting the IP address for 'www.commerce.net'. A Resolver then queries a net-server. The net-server responds with a request for the net-server's address and domain information. The Resolver then validates this domain information with the net-server. Next, the net-server provides the IP address and a signature (SIG). The Resolver then queries the net-server again for the IP address and SIG. The net-server responds with the IP address and SIG. Finally, the Resolver queries COMBRIDGE-GUYVER for the IP address and SIG, and COMBRIDGE-GUYVER responds with the IP address and SIG.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Galvin § 2.2:</p> <p>Galvin § 3: 3. Secure Domain Name System Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records managed by the DNS.</p> <p>Galvin § 3.1.3: Secure DNS Server Operation The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned.</p> <p>Galvin § 3.2: [S]uppose a user application needs the IP address of the host <u>www.commerce.net</u>. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address.</p> <p>Galvin § 3.2:</p> <pre> sequenceDiagram participant User participant Resolver participant RootServer as root-server participant NetServer as net-server Resolver->>User: www.commerce.net, get IP address Resolver->>RootServer: www.commerce.net, IP address RootServer-->>Resolver: rsk, net-server, net-server-addr, net-domain-pk, net-domain-sig Resolver->>Resolver: validate net-domain-pk Resolver->>NetServer: net, IP address NetServer-->>Resolver: IP address, SIG Resolver->>Resolver: validate IP address </pre> <p>...</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	<p>The diagram illustrates several network communication scenarios:</p> <ul style="list-style-type: none"> Scenario 1: A Resolver sends a request for 'www.commerce.net, IP address' to a 'not-server'. The server responds with 'ask commerce-server, commerce-server-addr, commerce-domain-pk, commerce-domain-sig'. A second Resolver then performs 'validate commerce-domain-pk'. Scenario 2: A Resolver sends a request for 'commerce.net, IP address' to a 'commerce-server'. The server responds with 'IP address, SIG'. A second Resolver then performs 'validate IP address'. Scenario 3: A Resolver sends a request for 'www.commerce.net, IP address' to a 'commerce-server'. The server responds with 'IP address, ip-address-sig'. A second Resolver then performs 'validate ip-address-sig'. Scenario 4: A User sends a request for 'www.commerce.net, IP address' to a Resolver.
<p>sending an access request message to the secure computer network address using a virtual private network</p>	<p>Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
communication link.	<p>Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication.</p> <p>Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.</p> <p>End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.</p> <p>Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.</p>
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	<p>Kaufman, Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.</p>

Appendix F
Citations to Exemplary Description in the Gauntlet Admin Guide Reference*

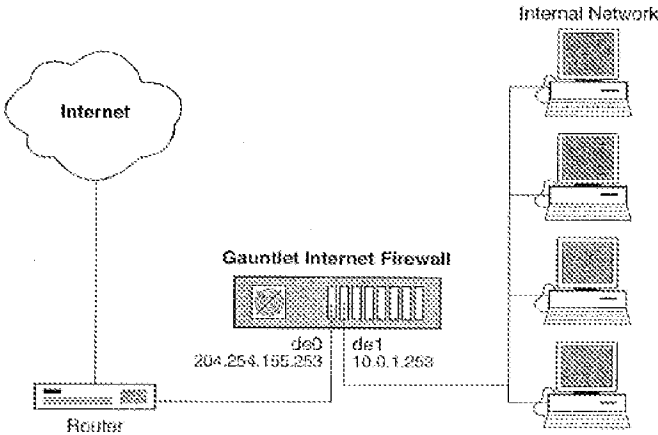
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>Page 1-9: The proxies also check to determine if the request is permitted for the destination. For some services, the proxies can perform the additional step of authenticating the user. This helps verify that users are who they say they are. The proxy then passes the request to the appropriate machine on the other side of the firewall using the standard protocol for that service.</p> <p>Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p> <p>Page 28-2: For example, consider the situation of a user, John, working at a client site (blaze.clientsite.com) who needs information stored on a machine at work (dimension.yoyodyne.com). When John tries to FTP to dimension, which is within the perimeter, he must authenticate at the firewall (fire-out.yoyodyne.com).</p> <p>The FTP proxy then prompts John for his authentication information (user name and password), which it verifies against the information in the user authentication database. If John provided the proper information, and his account is not disabled, the proxy provides a prompt. John can then connect to dimension on the inside network.</p> <p>Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.</p>

* - The cited passages are an indication of where in the Gauntlet reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

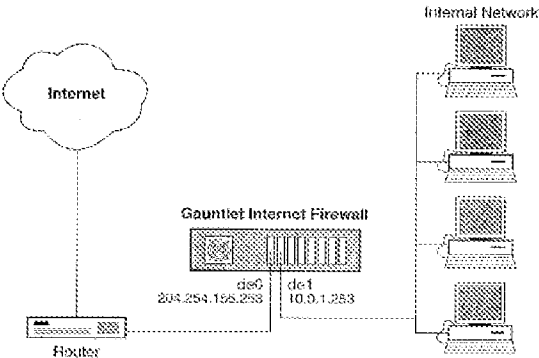
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference						
<p>receiving a secure domain name;</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.</p> <p>If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 934 1317 1161"> <thead> <tr> <th data-bbox="560 934 755 966">Parameters</th> <th data-bbox="755 934 1317 966">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 966 755 1066">IP Address & Mask</td> <td data-bbox="755 966 1317 1066">Enter the IP address of the machine to which you want to permit or deny access.</td> </tr> <tr> <td data-bbox="560 1066 755 1161">or Hostname</td> <td data-bbox="755 1066 1317 1161">Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u>.</td> </tr> </tbody> </table> <p>Note: You cannot use the asterisk (*) wildcard in this field.</p> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1: domain name system (DNS) The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</p>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access.	or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> .
Parameters	Enter						
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access.						
or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> .						

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 814 1317 1045"> <thead> <tr> <th data-bbox="560 814 755 850">Parameters</th> <th data-bbox="755 814 1317 850">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 850 755 947">IP Address & Mask</td> <td data-bbox="755 850 1317 947">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="560 947 755 1045">or Hostname</td> <td data-bbox="755 947 1317 1045">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1:</p> <table data-bbox="560 1129 1421 1232"> <tr> <td data-bbox="560 1129 885 1232">domain name system (DNS)</td> <td data-bbox="885 1129 1421 1232">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference						
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 814 1317 1045"> <thead> <tr> <th data-bbox="560 814 755 850">Parameters</th> <th data-bbox="755 814 1317 850">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 850 755 947">IP Address & Mask</td> <td data-bbox="755 850 1317 947">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="560 947 755 1045">or Hostname</td> <td data-bbox="755 947 1317 1045">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1: domain name system (DNS) The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</p>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.
Parameters	Enter						
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.						
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.						

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 1-7:</p>  <p>Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
<p>4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-4:</p>

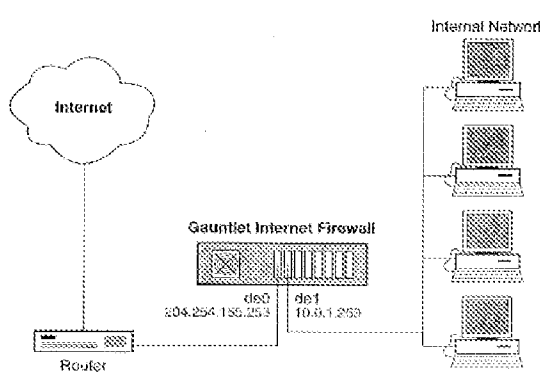
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference	
	Parameters	Enter
	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.
	or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> . Note: You cannot use the asterisk (*) wildcard in this field.
	<p>Pages 18-1 - 18-4: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>.....</p> <p>Configuring the firewall to allow PPTP traffic involves several steps that must be coordinated. You must configure:</p> <ul style="list-style-type: none"> The PPTP proxy to allow TCP Control connections Policies to allow the PPTP proxy Packet Screening to allow IP Data connections Packet Screening to absorb incoming TCP Control connections Routing on the PPTP client and server machines <p>.....</p> <p>Configuring the PPTP Proxy</p> <p>PPTP tunnels are initiated by client machines. Perform the following steps to configure the PPTP proxy to allow connections from all the desired clients.</p> <p>.....</p> <p>5. Provide information about the hosts that will communicate through the PPTP proxy.</p> <ul style="list-style-type: none"> - Enter the IP address and mask or the host name of the machine or network sending PPTP requests. The asterisk wildcard (*) is valid in host names. - Enter the IP address or host name of the hosts to which the PPTP proxy should connect. - Enter the port number of the remote host to which the PPTP proxy sends requests. The default port is 1723. - If desired, enter a description for your rule. <p>Page G-1: domain name system (DNS) The online distributed database system used to map human-readable</p>	

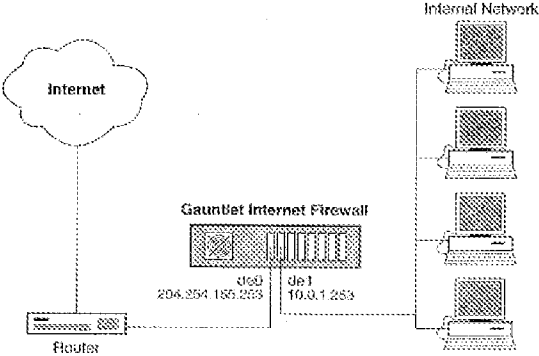
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	<p>machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</p>
<p>10. The method according to claim 1, wherein the virtual private network includes the Internet.</p>	<p>Page 1-7:</p>  <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'die0' with IP address '204.254.156.253' and 'die1' with IP address '10.0.1.253'. The 'die1' interface is connected to an 'Internal Network' which contains several computer icons.</p> <p>Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.</p>
<p>12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
<p>13. The method of claim 1, wherein receiving the secure domain</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
<p>name comprises receiving the secure domain name at a client computer from a user;</p>	<p>the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.</p> <p>If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 911 1317 1140"> <thead> <tr> <th data-bbox="560 911 755 940">Parameters</th> <th data-bbox="755 911 1317 940">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 940 755 1045">IP Address & Mask</td> <td data-bbox="755 940 1317 1045">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="560 1045 755 1140">or Hostname</td> <td data-bbox="755 1045 1317 1140">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1:</p> <table border="1" data-bbox="560 1234 1427 1329"> <tbody> <tr> <td data-bbox="560 1234 881 1329">domain name system (DNS)</td> <td data-bbox="881 1234 1427 1329">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </tbody> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that</p>								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
	<p>policy or proxy, the firewall passes on the request. Page 5-4:</p> <table border="1" data-bbox="560 653 1317 877"> <thead> <tr> <th data-bbox="560 653 751 684">Parameters</th> <th data-bbox="751 653 1317 684">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 684 751 783">IP Address & Mask</td> <td data-bbox="751 684 1317 783">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="560 783 751 877">or Hostname</td> <td data-bbox="751 783 1317 877">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing. Page G-1:</p> <table border="1" data-bbox="560 974 1427 1068"> <tr> <td data-bbox="560 974 889 1068">domain name system (DNS)</td> <td data-bbox="889 974 1427 1068">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall. Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request. Page 5-4:</p> <table border="1" data-bbox="560 1283 1317 1486"> <thead> <tr> <th data-bbox="560 1283 751 1314">Parameters</th> <th data-bbox="751 1283 1317 1314">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 1314 751 1413">IP Address & Mask</td> <td data-bbox="751 1314 1317 1413">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="560 1413 751 1486">or Hostname</td> <td data-bbox="751 1413 1317 1486">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.</td> </tr> </tbody> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu .		
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu .								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference		
	<p data-bbox="760 604 1317 632">Note: You cannot use the asterisk (*) wildcard in this field.</p> <p data-bbox="553 632 1446 701">Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p data-bbox="553 701 639 722">Page G-1:</p> <table border="1" data-bbox="565 722 1430 821"> <tr> <td data-bbox="565 722 841 751">domain name system (DNS)</td> <td data-bbox="846 722 1430 821">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.		
<p data-bbox="136 821 548 890">wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p data-bbox="553 821 634 842">Page 1-7:</p> <div data-bbox="574 869 1235 1304"> <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'eth0' with IP address '204.254.155.253' and 'eth1' with IP address '10.0.1.253'. The 'eth1' interface is connected to an 'Internal Network' which contains four computer icons.</p> </div> <p data-bbox="553 1325 1446 1436">Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p data-bbox="553 1436 1446 1484">The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops</p>		

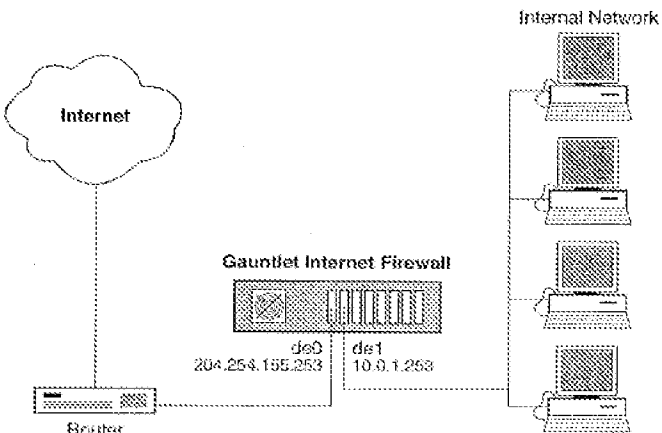
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
14. The method of claim 1, performed by a software module.	<p>See claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use).</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
15. The method of claim 1, performed by a client computer.	<p>See claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use).</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
17. A computer-readable storage medium, comprising:	<p>Page 1-7:</p>  <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'eth0' with IP address '204.254.136.253' and 'eth1' with IP address '10.0.1.253'. The 'eth1' interface is connected to an 'Internal Network' which contains several computer icons representing servers or clients.</p> <p>Page 10-1: There is a vast wealth of information stored on machines connected</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	<p>to the Internet.</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
<p>a storage area; and</p>	<p>Page 1-7:</p>  <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The Firewall has two interfaces: 'eth0' with IP address '206.254.186.253' and 'eth1' with IP address '193.1.253'. The Firewall is connected to an 'Internal Network' which contains several computer icons.</p> <p>Page 10-1: There is a vast wealth of information stored on machines connected to the Internet.</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
<p>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>Preface: In addition to this Administrators Guide, the following resources are available to help you understand and use your Gauntlet Firewall software:</p> <p>Page 1-9: The proxies also check to determine if the request is permitted for the destination. For some services, the proxies can perform the additional step of authenticating the user. This helps verify that users are who they say they are. The proxy then passes the request to the appropriate machine on the other side of the firewall using the standard protocol for that service.</p> <p>Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to</p>

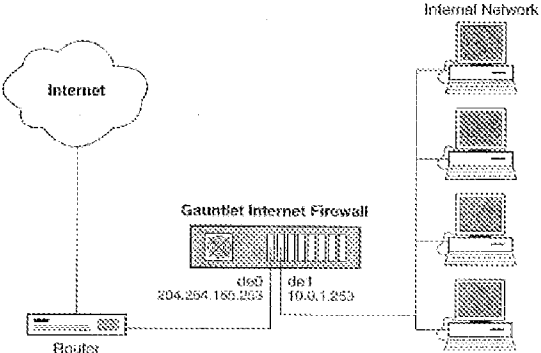
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference						
	<p>tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p> <p>Page 28-2: For example, consider the situation of a user, John, working at a client site (blaze.clientsite.com) who needs information stored on a machine at work (dimension.yoyodyne.com). When John tries to FTP to dimension, which is within the perimeter, he must authenticate at the firewall (fire-out.yoyodyne.com).</p> <p>The FTP proxy then prompts John for his authentication information (user name and password), which it verifies against the information in the user authentication database. If John provided the proper information, and his account is not disabled, the proxy provides a prompt. John can then connect to dimension on the inside network.</p> <p>Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.</p>						
<p>name; receiving a secure domain</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.</p> <p>If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.</p> <p>Page 5-4:</p> <table border="1" data-bbox="561 1314 1317 1493"> <thead> <tr> <th data-bbox="561 1314 760 1346">Parameters</th> <th data-bbox="760 1314 1317 1346">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="561 1346 760 1444">IP Address & Mask</td> <td data-bbox="760 1346 1317 1444">Enter the IP address of the machine to which you want to permit or deny access.</td> </tr> <tr> <td data-bbox="561 1444 760 1493">or Hostname</td> <td data-bbox="760 1444 1317 1493"> <p>Note: You cannot use the asterisk (*) wildcard in this field.</p> Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.</td> </tr> </tbody> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access.	or Hostname	<p>Note: You cannot use the asterisk (*) wildcard in this field.</p> Enter a hostname to which you want to permit or deny access, such as www.bigu.edu .
Parameters	Enter						
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access.						
or Hostname	<p>Note: You cannot use the asterisk (*) wildcard in this field.</p> Enter a hostname to which you want to permit or deny access, such as www.bigu.edu .						

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
	<table border="1" data-bbox="558 611 1317 657"> <tr> <td data-bbox="558 611 751 657"></td> <td data-bbox="756 611 1317 657">Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </table> <p data-bbox="553 657 1458 726">Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p data-bbox="553 726 643 747">Page G-1:</p> <table border="1" data-bbox="558 747 1430 846"> <tr> <td data-bbox="558 747 878 846">domain name system (DNS)</td> <td data-bbox="883 747 1430 846">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>		Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.				
	Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								
<p data-bbox="136 846 548 968">sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p data-bbox="553 846 1458 968">Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p data-bbox="553 968 1458 1037">Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p data-bbox="553 1037 643 1058">Page 5-4:</p> <table border="1" data-bbox="558 1058 1317 1287"> <thead> <tr> <th data-bbox="558 1058 751 1094">Parameters</th> <th data-bbox="756 1058 1317 1094">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="558 1094 751 1192">IP Address & Mask</td> <td data-bbox="756 1094 1317 1192">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="558 1192 751 1287">or Hostname</td> <td data-bbox="756 1192 1317 1287">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p data-bbox="553 1287 1458 1356">Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p data-bbox="553 1356 643 1377">Page G-1:</p> <table border="1" data-bbox="558 1377 1430 1474"> <tr> <td data-bbox="558 1377 878 1474">domain name system (DNS)</td> <td data-bbox="883 1377 1430 1474">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
<p>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 821 1317 1045"> <thead> <tr> <th data-bbox="560 821 753 850">Parameters</th> <th data-bbox="758 821 1317 850">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 856 753 947">IP Address & Mask</td> <td data-bbox="758 856 1317 947">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="560 953 753 1045">or Hostname</td> <td data-bbox="758 953 1317 1045">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1:</p> <table border="1" data-bbox="560 1142 1425 1226"> <tr> <td data-bbox="560 1142 841 1226">domain name system (DNS)</td> <td data-bbox="846 1142 1425 1226">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Page 1-7:</p>  <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'de0' with IP address '204.254.155.253' and 'de1' with IP address '10.0.1.253'. The 'de1' interface is connected to an 'Internal Network' which contains four computer icons.</p> <p>Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
<p>20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-4:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference			
	Parameters	Enter		
	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.		
	or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> . Note: You cannot use the asterisk (*) wildcard in this field.		
	<p>Pages 18-1 - 18-4: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>....</p> <p>Configuring the firewall to allow PPTP traffic involves several steps that must be coordinated. You must configure:</p> <ul style="list-style-type: none"> The PPTP proxy to allow TCP Control connections Policies to allow the PPTP proxy Packet Screening to allow IP Data connections Packet Screening to absorb incoming TCP Control connections Routing on the PPTP client and server machines <p>....</p> <p>Configuring the PPTP Proxy</p> <p>PPTP tunnels are initiated by client machines. Perform the following steps to configure the PPTP proxy to allow connections from all the desired clients.</p> <p>....</p> <p>5. Provide information about the hosts that will communicate through the PPTP proxy.</p> <ul style="list-style-type: none"> - Enter the IP address and mask or the host name of the machine or network sending PPTP requests. The asterisk wildcard (*) is valid in host names. - Enter the IP address or host name of the hosts to which the PPTP proxy should connect. - Enter the port number of the remote host to which the PPTP proxy sends requests. The default port is 1723. - If desired, enter a description for your rule. <p>Page G-1:</p> <table border="1" data-bbox="553 1465 1458 1493"> <tr> <td data-bbox="553 1465 841 1493">domain name system (DNS)</td> <td data-bbox="846 1465 1458 1493">The online distributed database system used to map human-readable</td> </tr> </table>		domain name system (DNS)	The online distributed database system used to map human-readable
domain name system (DNS)	The online distributed database system used to map human-readable			

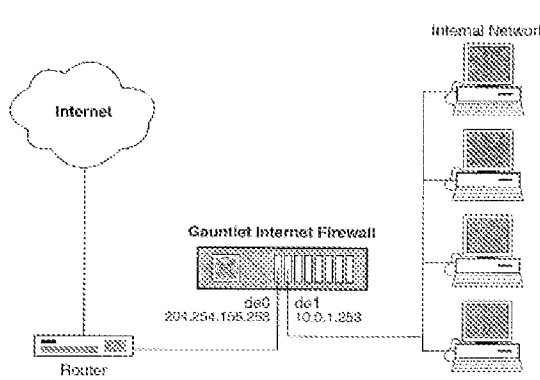
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference	
		machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
<p>26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.</p>	<p>Page 1-7:</p>  <p>Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.</p>	
<p>28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>	
<p>29. The computer-readable medium according to claim 17,</p>		

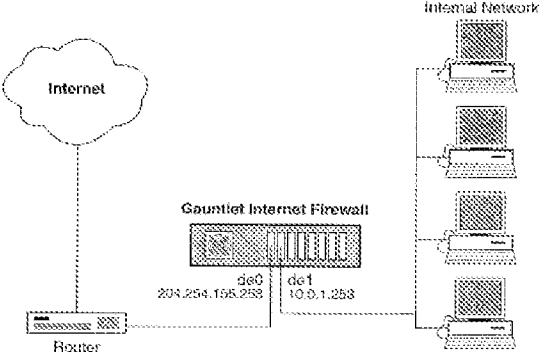
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
<p>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.</p> <p>If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 934 1315 1165"> <thead> <tr> <th data-bbox="560 934 755 966">Parameters</th> <th data-bbox="755 934 1315 966">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 966 755 1060">IP Address & Mask</td> <td data-bbox="755 966 1315 1060">Enter the IP address of the machine to which you want to permit or deny access.</td> </tr> <tr> <td data-bbox="560 1060 755 1165">or Hostname</td> <td data-bbox="755 1060 1315 1165">Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u>.</td> </tr> </tbody> </table> <p>Note: You cannot use the asterisk (*) wildcard in this field.</p> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1:</p> <table border="1" data-bbox="560 1249 1429 1354"> <tr> <td data-bbox="560 1249 876 1354">domain name system (DNS)</td> <td data-bbox="876 1249 1429 1354">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access.	or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> .	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> .								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the</p>								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
	<p>request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request. Page 5-4:</p> <table border="1" data-bbox="560 674 1317 905"> <thead> <tr> <th>Parameters</th> <th>Enter</th> </tr> </thead> <tbody> <tr> <td>IP Address & Mask</td> <td>Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td>or Hostname</td> <td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing. Page G-1:</p> <table border="1" data-bbox="560 999 1425 1094"> <tr> <td>domain name system (DNS)</td> <td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.								
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall. Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request. Page 5-4:</p> <table border="1" data-bbox="560 1308 1317 1486"> <thead> <tr> <th>Parameters</th> <th>Enter</th> </tr> </thead> <tbody> <tr> <td>IP Address & Mask</td> <td>Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td>or Hostname</td> <td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.</td> </tr> </tbody> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu .		
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu .								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference		
	<p data-bbox="760 632 1252 653">Note: You cannot use the asterisk (*) wildcard in this field.</p> <p data-bbox="553 657 1446 726">Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p data-bbox="553 730 639 747">Page G-1:</p> <table border="1" data-bbox="553 751 1430 842"> <tr> <td data-bbox="553 751 841 779">domain name system (DNS)</td> <td data-bbox="846 751 1430 842">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.		
<p data-bbox="136 852 529 921">wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p data-bbox="553 852 634 869">Page 1-7:</p> <div data-bbox="574 898 1230 1329"> <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'de0' with IP address '204.254.155.253' and 'de1' with IP address '10.0.1.253'. The 'de1' interface is connected to an 'Internal Network' which contains four computer icons.</p> </div> <p data-bbox="553 1350 1446 1465">Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p data-bbox="553 1470 1430 1484">The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server</p>		

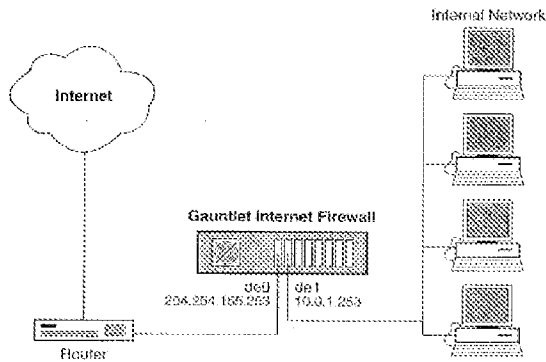
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	<p>See claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use).</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	<p>See claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use).</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
<p>33. A data processing apparatus, comprising:</p>	<p>Page 1-7:</p>  <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'de0' with IP address '204.254.195.258' and 'de1' with IP address '10.0.1.253'. The 'de1' interface is connected to an 'Internal Network' which contains several computer icons.</p> <p>Page 1-8: Processing packets and requests The firewall follows a standard set of steps for the packets it receives:</p> <ol style="list-style-type: none"> 1. Receive packet 2. Check source and destination 3. Check request type 4. Call appropriate program 5. Process the request <p>As we examine each step of the process, consider a Yoyodyne employee working at a client site (outside the perimeter) who needs access to her machine at work via TELNET.</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
<p>a processor, and</p>	<p>Page 1-7:</p>  <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'de0' with IP address '204.254.195.253' and 'de1' with IP address '10.0.1.253'. The 'de1' interface is connected to an 'Internal Network' which contains several computer icons.</p> <p>Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>
<p>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>Preface: In addition to this Administrators Guide, the following resources are available to help you understand and use your Gauntlet Firewall software:</p> <p>Page 1-1: The Gauntlet Firewall is a software-based firewall system that provides secure access and internetwork communications between private networks and public networks (such as the Internet), and between subnets of private networks. The firewall offers application-level security services for both incoming and outgoing communications based on existing security practices or an organization's security policies.</p> <p>Page 1-4: The software on the Gauntlet Firewall includes security services for a number of popular applications. Each application generally talks through a different proxy that understands the protocol for that application.</p> <p>Page 1-7:</p>

7,188,180 Claim Elements

Description for Claimed Elements in the Gauntlet Prior Art Reference



Page 1-9: The proxies also check to determine if the request is permitted for the destination. For some services, the proxies can perform the additional step of authenticating the user. This helps verify that users are who they say they are. The proxy then passes the request to the appropriate machine on the other side of the firewall using the standard protocol for that service.

Page 7-6:

The following table describes FTP operations.

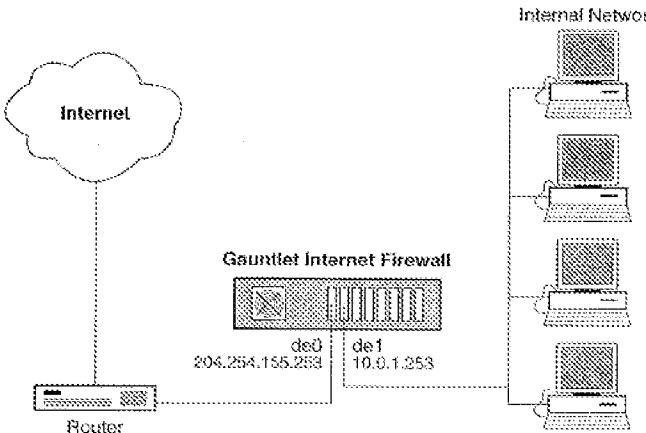
FTP Operation	Description
CWD/CDUP	Change working directory.
DELE	Delete a file.
LIST/NLIST	List files in a directory.
MKD	Make a directory.
RETR	Retrieve a file.
RMD	Remove a directory.
STOR/STOU	Store or copy a file.
SITE	Access commands supported by site request such as request, unmask, idle, and chmod.

Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference								
	<p>Page 28-2: For example, consider the situation of a user, John, working at a client site (blaze.clientsite.com) who needs information stored on a machine at work (dimension.yoyodyne.com). When John tries to FTP to dimension, which is within the perimeter, he must authenticate at the firewall (fire-out.yoyodyne.com).</p> <p>The FTP proxy then prompts John for his authentication information (user name and password), which it verifies against the information in the user authentication database. If John provided the proper information, and his account is not disabled, the proxy provides a prompt. John can then connect to dimension on the inside network.</p>								
<p>receiving a secure domain name;</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.</p> <p>If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 1102 1315 1333"> <thead> <tr> <th data-bbox="560 1102 755 1134">Parameters</th> <th data-bbox="755 1102 1315 1134">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 1134 755 1228">IP Address & Mask</td> <td data-bbox="755 1134 1315 1228"> Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field. </td> </tr> <tr> <td data-bbox="560 1228 755 1333">or Hostname</td> <td data-bbox="755 1228 1315 1333"> Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field. </td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1:</p> <table border="1" data-bbox="560 1417 1429 1495"> <tr> <td data-bbox="560 1417 876 1495">domain name system (DNS)</td> <td data-bbox="876 1417 1429 1495">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace</td> </tr> </table>	Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace
Parameters	Enter								
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.								
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.								
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace								

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference									
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>that allows sites to assign machine names and addresses.</p> <p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-4:</p> <table border="1" data-bbox="561 844 1317 1073"> <thead> <tr> <th data-bbox="561 844 753 873">Parameters</th> <th data-bbox="760 844 1317 873">Enter</th> </tr> </thead> <tbody> <tr> <td data-bbox="561 877 753 974">IP Address & Mask</td> <td data-bbox="760 877 1317 974">Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> <tr> <td data-bbox="561 978 753 1073">or Hostname</td> <td data-bbox="760 978 1317 1073">Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. Note: You cannot use the asterisk (*) wildcard in this field.</td> </tr> </tbody> </table> <p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1:</p> <table border="1" data-bbox="561 1167 1425 1260"> <tr> <td data-bbox="561 1167 889 1260">domain name system (DNS)</td> <td data-bbox="896 1167 1425 1260">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>		Parameters	Enter	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.	or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.	domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
Parameters	Enter									
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.									
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu . Note: You cannot use the asterisk (*) wildcard in this field.									
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.									
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.</p> <p>Page 5-4:</p>									

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference			
	<table border="1"> <thead> <tr> <th data-bbox="545 604 753 636">Parameters</th> <th data-bbox="753 604 1317 636">Enter</th> </tr> </thead> </table>	Parameters	Enter	
	Parameters	Enter		
	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.		
or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> . Note: You cannot use the asterisk (*) wildcard in this field.			
<p>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.</p> <p>Page G-1:</p> <table border="1"> <tr> <td data-bbox="545 926 841 1024">domain name system (DNS)</td> <td data-bbox="841 926 1317 1024">The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td> </tr> </table>		domain name system (DNS)		The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.			
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 1-7:			

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference				
	 <p>The diagram illustrates a network configuration. On the left, a cloud labeled 'Internet' is connected to a 'Router'. The Router is connected to the 'Gauntlet Internet Firewall'. The firewall has two interfaces: 'de0' with IP address '204.254.155.253' and 'de1' with IP address '10.0.1.253'. The 'de1' interface is connected to an 'Internal Network' which contains four laptops.</p> <p>Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.</p>				
<p>35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.</p> <p>Page 5-4:</p> <table border="1" data-bbox="560 1459 1315 1491"> <thead> <tr> <th>Parameters</th> <th>Enter</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Parameters	Enter		
Parameters	Enter				

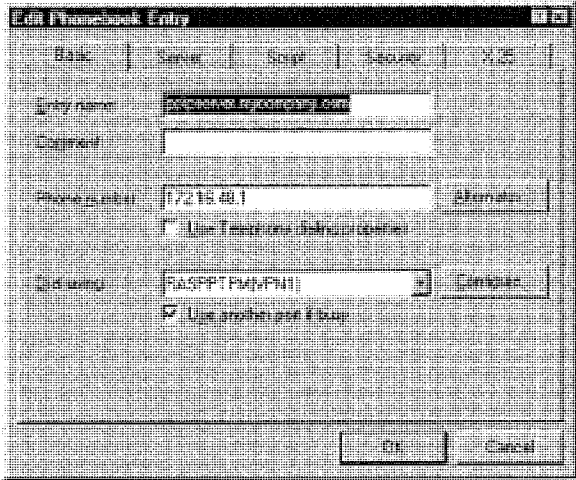
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference	
	IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. Note: You cannot use the asterisk (*) wildcard in this field.
	or Hostname	Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u> . Note: You cannot use the asterisk (*) wildcard in this field.
	<p>Pages 18-1 - 18-4: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.</p> <p>.....</p> <p>Configuring the firewall to allow PPTP traffic involves several steps that must be coordinated. You must configure:</p> <ul style="list-style-type: none"> The PPTP proxy to allow TCP Control connections Policies to allow the PPTP proxy Packet Screening to allow IP Data connections Packet Screening to absorb incoming TCP Control connections Routing on the PPTP client and server machines <p>.....</p> <p>Configuring the PPTP Proxy</p> <p>PPTP tunnels are initiated by client machines. Perform the following steps to configure the PPTP proxy to allow connections from all the desired clients.</p> <p>.....</p> <p>5. Provide information about the hosts that will communicate through the PPTP proxy.</p> <ul style="list-style-type: none"> - Enter the IP address and mask or the host name of the machine or network sending PPTP requests. The asterisk wildcard (*) is valid in host names. - Enter the IP address or host name of the hosts to which the PPTP proxy should connect. - Enter the port number of the remote host to which the PPTP proxy sends requests. The default port is 1723. - If desired, enter a description for your rule. 	
	Page G-1: domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	assign machine names and addresses.

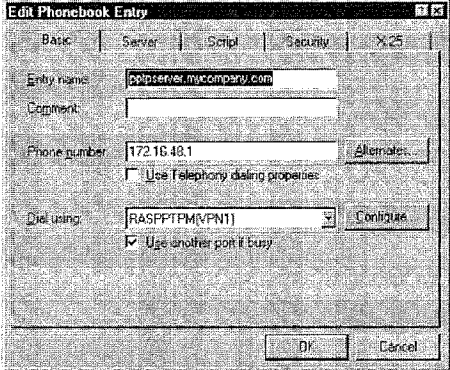
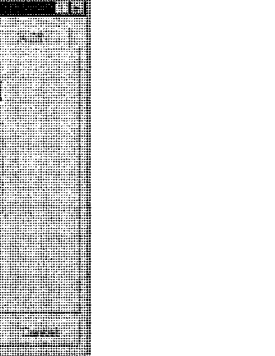
Appendix G
Citations to Exemplary Description in the Hands On and Installing NT References*

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet.”</p> <p>Hands On Page 432: <i>Security</i>. PPTP provides security through data encryption. A PPTP connection over the Internet is encrypted and works with the NetBEUI, TCP/IP, and IPX protocols. Data sent by means of a PPTP tunnel consists of encapsulated PPP packets. If Dial-Up Networking is configured to use data encryption, the data sent by means of PPTP is encrypted when sent.</p> <p>Hands On, Page 435: The Point-to-Point Protocol (PPP) was designed as an enhancement to the original SLIP specification. PPP is a set of industry standard framing and authentication protocols that enable RAS clients and servers to interoperate in a multivendor network.</p> <p>Hands On Page 438: Windows NT Server provides for enterprise-wide security using a trusted domain, single-network logon model. This eliminates the need for duplicate user accounts across a multiple-server network. The single-network logon model extends to RAS users. The RAS server uses the same user account database as the computer running Windows NT. This allows easier administration, because clients can log on with the same user accounts that they use at the office. This feature ensures that clients have the same privileges and permissions they ordinarily have while in the office.</p> <p>To connect to a RAS server, clients must have a valid Windows NT user account as well as the RAS dial-in permission. Clients must first be authenticated by RAS before they can log on to Windows NT.</p> <p>Hands On Page 447:</p> <p>Encryption settings Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients.</p> <p>If Required Microsoft encrypted authentication is selected, Require data encryption can also be selected.</p> <p>Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.</p>
<p>receiving a secure domain name;</p>	<p>Installing NT Pages 20 - 21:</p> <p>5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the Phone Number dialog box.</p> <p>Note If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.</p>

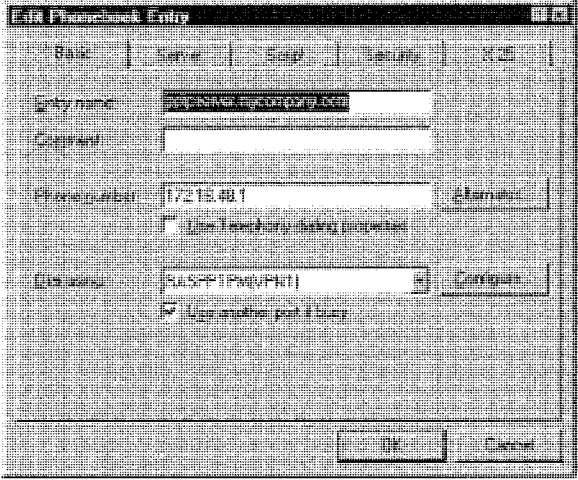
* - The cited passages are an indication of where in the Hands On and Installing NT references, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 <p data-bbox="488 1102 992 1123"><i>Figure 12 - Example Phonebook entry for PPTP server and a VPN device</i></p>
<p data-bbox="147 1157 440 1318">sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p data-bbox="456 1157 1456 1203">Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <ol data-bbox="508 1203 1456 1297" style="list-style-type: none"> <li data-bbox="508 1203 1044 1226">1. A resolver (or client) passes a query to its local name server. <li data-bbox="508 1226 1456 1272">2. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. <li data-bbox="508 1272 1333 1297">3. When the local name server has the address requested, it returns the information to the resolver. <p data-bbox="456 1297 1456 1344">Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p data-bbox="456 1344 1456 1390">Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p data-bbox="456 1390 1456 1486">The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>
<p data-bbox="224 1486 440 1507">receiving from the secure</p>	<p data-bbox="456 1486 1456 1507">Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific</p>

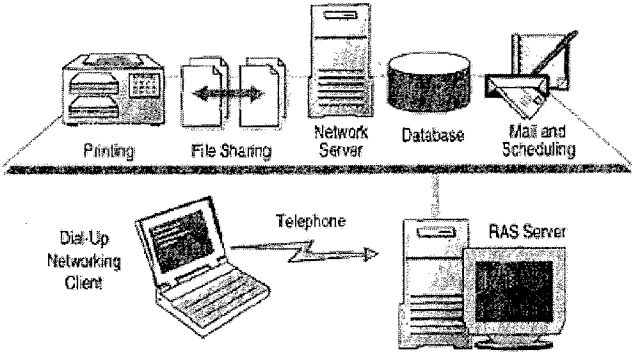
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>IP address. The name resolution process is outlined below:</p> <ol style="list-style-type: none"> 1. A resolver (or client) passes a query to its local name server. 2. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 3. When the local name server has the address requested, it returns the information to the resolver. <p>Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p>Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p>The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."</p>
<p>4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.</p> <p>Installing NT Page 20: Creating the Phonebook Entry to Dial a PPTP Server You must create a phonebook entry to connect to your PPTP server by using a VPN device.</p> <p>....</p> <p>5: Type the IP address of the adapter on the PPTP server that is connected to the Internet in the Phone Number dialog box.</p> <p>Installing NT Page 21:</p> <p>Note</p> <p>If your PPTP server has an Internet registered DNS name, you could alternatively enter it's DNS name in this field.</p> <p>....</p> <p><i>To verify or edit your phonebook entry for the PPTP server</i></p> <ol style="list-style-type: none"> 1. Click More in Dial-Up Networking, and then click Edit entry and modem properties to verify that your PPTP server phonebook entry is correctly configured. The Edit Phonebook Entry dialog box will appear as illustrated in the following figure.

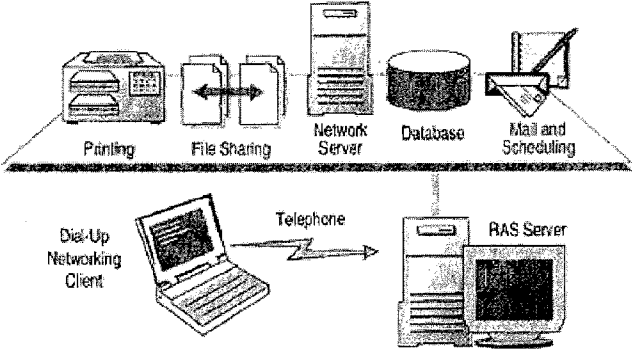
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 <p data-bbox="467 989 860 1008"><i>Figure 12 - Example Phonebook entry for PPTP server and a VPN device</i></p> <p data-bbox="467 1016 649 1035">Installing NT Page 22:</p>  <p data-bbox="467 1419 849 1438"><i>Figure 13 - Verifying the Dial-Up Server configuration on the PPTP client</i></p> <p data-bbox="467 1457 500 1476">....</p> <p data-bbox="467 1476 505 1495">Note</p> <p data-bbox="467 1495 1450 1514">If you are configuring the VPN device on an ISP server running Windows NT Server version 4.0 that is configured with</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	<p>multiple VPN devices, repeat this procedure for each VPN device.</p> <p>Installing NT Page 23: A PPTP-enabled client must have two phonebook entries (as described in the previous section) to connect to a PPTP server.</p> <p>.....</p> <p>After successful connection, all traffic through your modem is routed by the ISP over the Internet to your PPTP server, which routes the traffic to the correct computer.</p> <p>Installing NT Page 24: You do not need to make a second dial-up call because the ISP server configured as a PPTP client, makes the connection to the PPTP server for the PPP client.</p>
<p>10. The method according to claim 1, wherein the virtual private network includes the Internet.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."</p>
<p>12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."</p>
<p>13. The method of claim 1, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Installing NT Pages 20 - 21:</p> <p>5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the Phone Number dialog box.</p> <p>Note If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.</p>

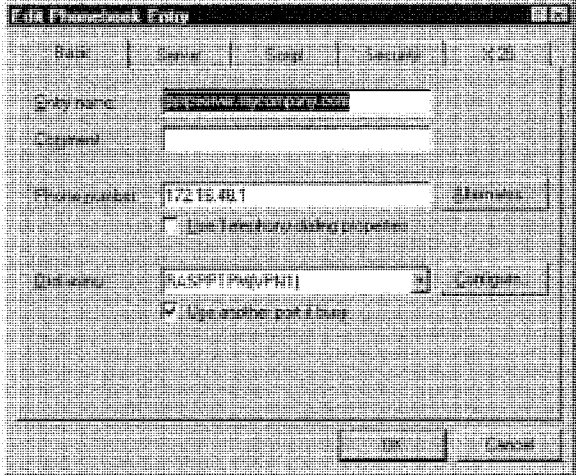
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 <p data-bbox="488 1100 992 1121"><i>Figure 12 - Example Phonebook entry for PPTP server and a VPN device</i></p>
<p data-bbox="147 1157 431 1247">wherein sending the query message comprises sending the query message at the client computer;</p>	<p data-bbox="456 1157 1442 1199">Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <ol data-bbox="509 1203 1446 1293" style="list-style-type: none"> <li data-bbox="509 1203 1040 1224">4. A resolver (or client) passes a query to its local name server. <li data-bbox="509 1228 1446 1270">5. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. <li data-bbox="509 1274 1333 1295">6. When the local name server has the address requested, it returns the information to the resolver. <p data-bbox="456 1297 1455 1339">Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p data-bbox="456 1344 1442 1386">Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p data-bbox="456 1390 1446 1480">The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <ol style="list-style-type: none"> 4. A resolver (or client) passes a query to its local name server. 5. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 6. When the local name server has the address requested, it returns the information to the resolver. <p>Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p>Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p>The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."</p>
<p>14. The method of claim 1, performed by a software module.</p>	<p>See claim 1, which is performed by Windows NT 4.0.</p>
<p>15. The method of claim 1, performed by a client computer.</p>	<p>See claim 1, which is performed by Windows NT 4.0 installed and configured at the client computer.</p>
<p>17. A computer-readable storage medium, comprising:</p>	<p>Hands On Page 428:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	<p>The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client.</p> <ul style="list-style-type: none"> ■ WAN Connectivity ■ Remote Access Protocols ■ Gateways and Routers ■ Point-to-Point Tunneling Protocol (PPTP) ■ RAS Security Features  <p>The diagram shows a 'Dial-Up Networking Client' (represented by a laptop) connected to a 'RAS Server' (represented by a tower PC and monitor) via a 'Telephone' line. The RAS Server is connected to a 'Network Server' (represented by a tower PC). The Network Server is connected to several resources: 'Printing' (represented by a printer), 'File Sharing' (represented by two folders with a double-headed arrow), 'Database' (represented by a cylinder), and 'Mail and Scheduling' (represented by a calendar icon).</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>a storage area; and</p>	<p>Hands On Page 428:</p> <p>The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client.</p> <ul style="list-style-type: none"> ■ WAN Connectivity ■ Remote Access Protocols ■ Gateways and Routers ■ Point-to-Point Tunneling Protocol (PPTP) ■ RAS Security Features  <p>The diagram illustrates a Dial-Up Networking Client (a laptop) connected to a RAS Server (a computer tower and monitor) via a Telephone. The RAS Server is connected to a local network. This network includes a Printer, File Sharing (represented by two folders with a double-headed arrow), a Network Server (a tower PC), a Database (a cylinder), and Mail and Scheduling (a calendar icon).</p>
<p>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet.”</p> <p>Hands On Page 432: <i>Security</i>. PPTP provides security through data encryption. A PPTP connection over the Internet is encrypted and works with the NetBEUI, TCP/IP, and IPX protocols. Data sent by means of a PPTP tunnel consists of encapsulated PPP packets. If Dial-Up Networking is configured to use data encryption, the data sent by means of PPTP is encrypted when sent.</p> <p>Hands On Page 435: The Point-to-Point Protocol (PPP) was designed as an enhancement to the original SLIP specification. PPP is a set of industry standard framing and authentication protocols that enable RAS clients and servers to interoperate in a multivendor network.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References				
	<p>Hands On Page 438: Windows NT Server provides for enterprise-wide security using a trusted domain, single-network logon model. This eliminates the need for duplicate user accounts across a multiple-server network. The single-network logon model extends to RAS users. The RAS server uses the same user account database as the computer running Windows NT. This allows easier administration, because clients can log on with the same user accounts that they use at the office. This feature ensures that clients have the same privileges and permissions they ordinarily have while in the office.</p> <p>To connect to a RAS server, clients must have a valid Windows NT user account as well as the RAS dial-in permission. Clients must first be authenticated by RAS before they can log on to Windows NT.</p> <p>Hands On Page 447:</p> <table border="0" data-bbox="457 840 1412 961"> <tr> <td style="vertical-align: top;">Encryption settings</td> <td>Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients.</td> </tr> <tr> <td></td> <td>If Required Microsoft encrypted authentication is selected, Require data encryption can also be selected.</td> </tr> </table> <p>Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.</p>	Encryption settings	Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients.		If Required Microsoft encrypted authentication is selected, Require data encryption can also be selected.
Encryption settings	Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients.				
	If Required Microsoft encrypted authentication is selected, Require data encryption can also be selected.				
receiving a secure domain name;	<p>Installing NT Pages 20 - 21:</p> <p>5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the Phone Number dialog box.</p> <p>Note If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.</p>				

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 <p data-bbox="488 1098 992 1119"><i>Figure 12 - Example Phonebook entry for PPTP server and a VPN device</i></p>
<p data-bbox="147 1152 440 1314">sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p data-bbox="456 1152 1442 1199">Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <ol data-bbox="509 1199 1446 1289" style="list-style-type: none"> <li data-bbox="509 1199 1040 1220">7. A resolver (or client) passes a query to its local name server. <li data-bbox="509 1220 1446 1266">8. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. <li data-bbox="509 1266 1333 1289">9. When the local name server has the address requested, it returns the information to the resolver. <p data-bbox="456 1289 1455 1337">Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p data-bbox="456 1337 1442 1383">Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p data-bbox="456 1383 1446 1478">The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <ol style="list-style-type: none"> 7. A resolver (or client) passes a query to its local name server. 8. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 9. When the local name server has the address requested, it returns the information to the resolver. <p>Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p>Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p>The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."</p>
<p>20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.</p> <p>Installing NT Page 20: Creating the Phonebook Entry to Dial a PPTP Server You must create a phonebook entry to connect to your PPTP server by using a VPN device.</p> <p>....</p> <p>5: Type the IP address of the adapter on the PPTP server that is connected to the Internet in the Phone Number dialog box.</p> <p>Installing NT Page 21: Note If your PPTP server has an Internet registered DNS name, you could alternatively enter it's DNS name in this field.</p> <p>....</p> <p><i>To verify or edit your phonebook entry for the PPTP server</i></p> <ol style="list-style-type: none"> 1. Click More in Dial-Up Networking, and then click Edit entry and modem properties to verify that your PPTP server phonebook entry is correctly configured. The Edit Phonebook Entry dialog box will appear as illustrated in the following figure.

7,188,180 Claim Elements

Description for Claimed Elements in the Hands On and Installing NT Prior Art References

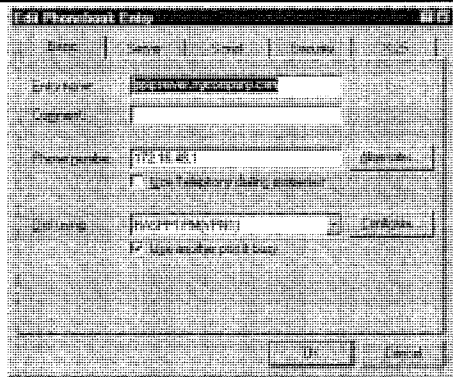


Figure 12 - Example Phonebook entry for PPTP server and a VPN device

Installing NT Page 22:

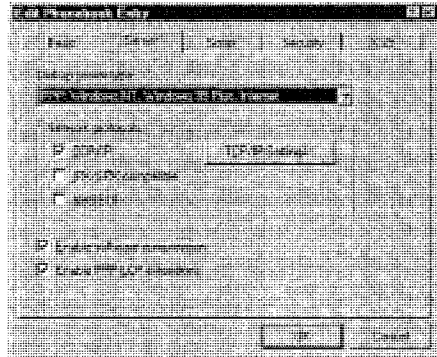
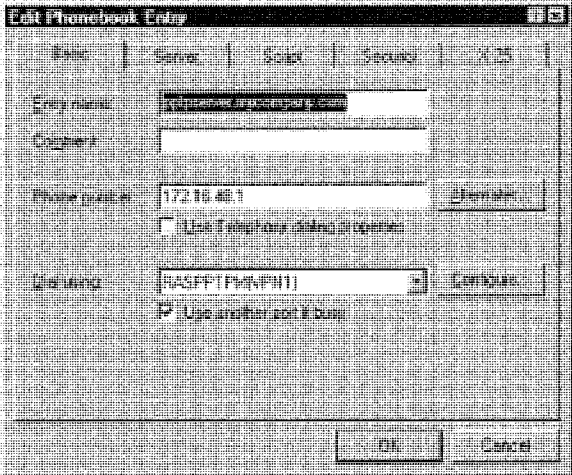


Figure 13 - Verifying the Dial-Up Server configuration on the PPTP client

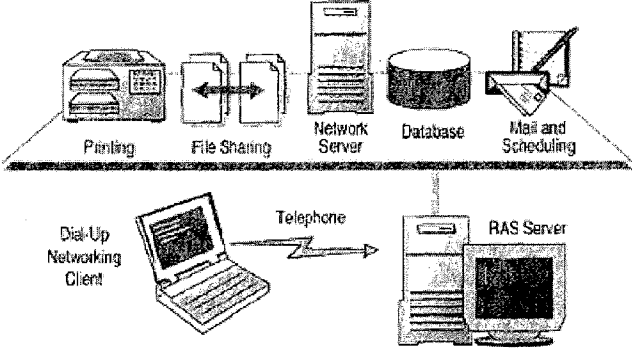
.....
Note

If you are configuring the VPN device on an ISP server running Windows NT Server version 4.0 that is configured with

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	<p>multiple VPN devices, repeat this procedure for each VPN device.</p> <p>Installing NT Page 23: A PPTP-enabled client must have two phonebook entries (as described in the previous section) to connect to a PPTP server.</p> <p>.....</p> <p>After successful connection, all traffic through your modem is routed by the ISP over the Internet to your PPTP server, which routes the traffic to the correct computer.</p> <p>Installing NT Page 24: You do not need to make a second dial-up call because the ISP server configured as a PPTP client, makes the connection to the PPTP server for the PPP client.</p>
<p>26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet.”</p>
<p>28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet.”</p>
<p>29. The computer-readable medium according to claim 17, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>Installing NT Pages 20 - 21:</p> <p>5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the Phone Number dialog box.</p> <p>Note If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.</p>

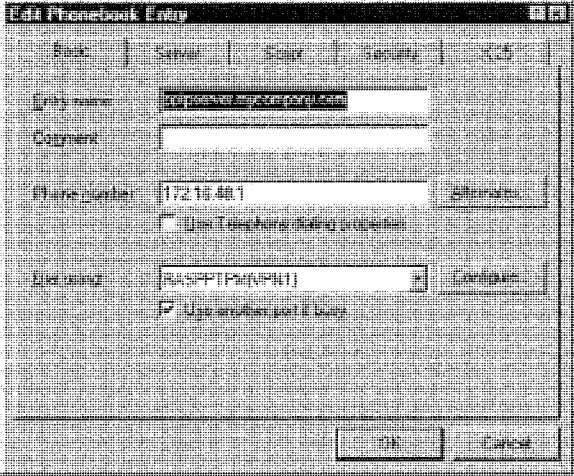
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 <p data-bbox="492 1098 992 1119"><i>Figure 12 - Example Phonebook entry for PPTP server and a VPN device</i></p>
<p data-bbox="147 1152 435 1245">wherein sending the query message comprises sending the query message at the client computer;</p>	<p data-bbox="456 1152 1442 1199">Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <ol style="list-style-type: none"> <li data-bbox="509 1199 1044 1220">10. A resolver (or client) passes a query to its local name server. <li data-bbox="509 1220 1446 1266">11. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. <li data-bbox="509 1266 1333 1287">12. When the local name server has the address requested, it returns the information to the resolver. <p data-bbox="456 1287 1455 1333">Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p data-bbox="456 1333 1442 1379">Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p data-bbox="456 1379 1446 1478">The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <p>10. A resolver (or client) passes a query to its local name server.</p> <p>11. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver.</p> <p>12. When the local name server has the address requested, it returns the information to the resolver.</p> <p>Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p>Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p>The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."</p>
<p>30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.</p>	<p>See claim 1, which is performed by Windows NT 4.0.</p>
<p>31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.</p>	<p>See claim 1, which is performed by Windows NT 4.0 installed and configured at the client computer.</p>

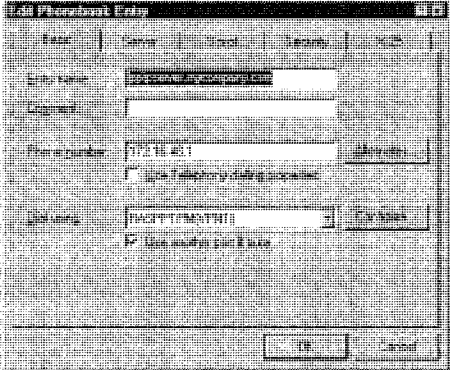
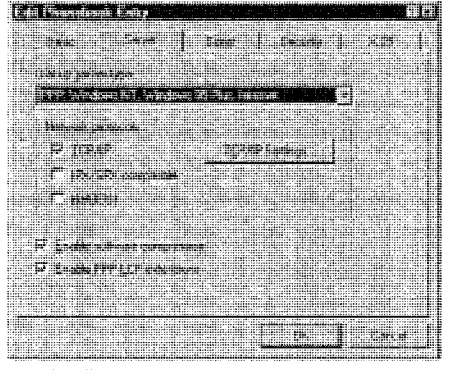
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>33. A data processing apparatus, comprising:</p>	<p>Hands On Page 428:</p> <p>The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client.</p> <ul style="list-style-type: none"> ■ WAN Connectivity ■ Remote Access Protocols ■ Gateways and Routers ■ Point-to-Point Tunneling Protocol (PPTP) ■ RAS Security Features  <p>The diagram shows a 'Dial-Up Networking Client' (represented by a laptop) connected to a 'RAS Server' (represented by a desktop computer) via a 'Telephone' line. The RAS Server is connected to a local network. This network includes a 'Network Server', a 'Database', 'Mail and Scheduling', 'File Sharing', and 'Printing' services. The 'Network Server' is connected to the 'RAS Server'. The 'Database' is connected to the 'Network Server'. The 'Mail and Scheduling' service is connected to the 'Network Server'. The 'File Sharing' service is connected to the 'Network Server'. The 'Printing' service is connected to the 'Network Server'.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>a processor, and</p>	<p>Hands On Page 428:</p> <p>The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client.</p> <ul style="list-style-type: none"> ■ WAN Connectivity ■ Remote Access Protocols ■ Gateways and Routers ■ Point-to-Point Tunneling Protocol (PPTP) ■ RAS Security Features

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet.”</p> <p>Hands On Page 432: <i>Security</i>. PPTP provides security through data encryption. A PPTP connection over the Internet is encrypted and works with the NetBEUI, TCP/IP, and IPX protocols. Data sent by means of a PPTP tunnel consists of encapsulated PPP packets. If Dial-Up Networking is configured to use data encryption, the data sent by means of PPTP is encrypted when sent.</p> <p>Hands On Page 435: The Point-to-Point Protocol (PPP) was designed as an enhancement to the original SLIP specification. PPP is a set of industry standard framing and authentication protocols that enable RAS clients and servers to interoperate in a multivendor network.</p> <p>Hands On Page 438: Windows NT Server provides for enterprise-wide security using a trusted domain, single-network logon model. This eliminates the need for duplicate user accounts across a multiple-server network. The single-network logon model extends to RAS users. The RAS server uses the same user account database as the computer running Windows NT. This allows easier administration, because clients can log on with the same user accounts that they use at the office. This feature ensures that clients have the same privileges and permissions they ordinarily have while in the office.</p> <p>To connect to a RAS server, clients must have a valid Windows NT user account as well as the RAS dial-in permission. Clients must first be authenticated by RAS before they can log on to Windows NT.</p> <p>Hands On Page 447:</p> <p>Encryption settings Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients.</p> <p>If Required Microsoft encrypted authentication is selected, Require data encryption can also be selected.</p> <p>Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.</p>
<p>receiving a secure domain name;</p>	<p>Installing NT Pages 20 - 21:</p> <p>5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the Phone Number dialog box.</p> <p>Note If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.</p>

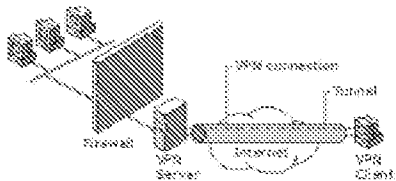
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 <p data-bbox="492 1104 992 1125"><i>Figure 12 - Example Phonebook entry for PPTP server and a VPN device</i></p> <p data-bbox="459 1131 1451 1178">Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.</p>
<p data-bbox="147 1182 443 1346">sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p data-bbox="459 1182 1451 1228">Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <ol style="list-style-type: none"> <li data-bbox="509 1230 1040 1251">13. A resolver (or client) passes a query to its local name server. <li data-bbox="509 1253 1451 1299">14. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. <li data-bbox="509 1302 1333 1323">15. When the local name server has the address requested, it returns the information to the resolver. <p data-bbox="459 1325 1451 1371">Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p data-bbox="459 1373 1451 1419">Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p data-bbox="459 1421 1451 1507">The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below:</p> <p>13. A resolver (or client) passes a query to its local name server.</p> <p>14. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver.</p> <p>15. When the local name server has the address requested, it returns the information to the resolver.</p> <p>Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality.</p> <p>Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line.</p> <p>The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."</p>
<p>35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.</p>	<p>Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.</p> <p>Installing NT Page 20: Creating the Phonebook Entry to Dial a PPTP Server You must create a phonebook entry to connect to your PPTP server by using a VPN device.</p> <p>....</p> <p>5: Type the IP address of the adapter on the PPTP server that is connected to the Internet in the Phone Number dialog box.</p> <p>Installing NT Page 21: Note If your PPTP server has an Internet registered DNS name, you could alternatively enter it's DNS name in this field.</p> <p>....</p> <p><i>To verify or edit your phonebook entry for the PPTP server</i></p> <p>1. Click More in Dial-Up Networking, and then click Edit entry and modem properties to verify that your PPTP server phonebook entry is correctly configured. The Edit Phonebook Entry dialog box will appear as illustrated in the following figure.</p>

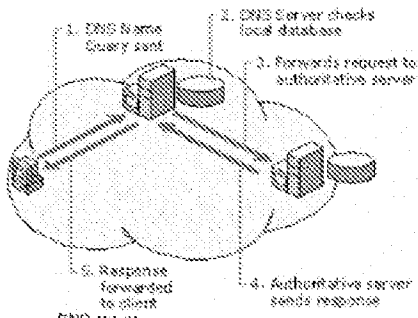
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 <p data-bbox="467 989 914 1010"><i>Figure 12 - Example Phonebook entry for PPTP server and a VPN device</i></p> <p data-bbox="467 1016 649 1037">Installing NT Page 22:</p>  <p data-bbox="467 1423 914 1444"><i>Figure 13 - Verifying the Dial-Up Server configuration on the PPTP client</i></p> <p data-bbox="467 1451 503 1472">.....</p> <p data-bbox="467 1478 503 1499">Note</p> <p data-bbox="467 1505 1466 1526">If you are configuring the VPN device on an ISP server running Windows NT Server version 4.0 that is configured with</p>

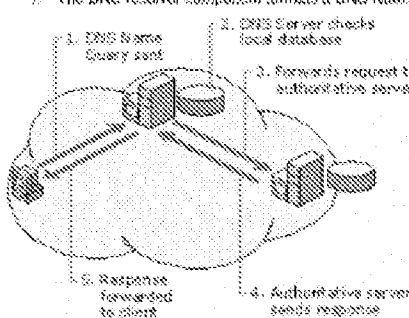
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	<p>multiple VPN devices, repeat this procedure for each VPN device.</p> <p>Installing NT Page 23: A PPTP-enabled client must have two phonebook entries (as described in the previous section) to connect to a PPTP server.</p> <p>....</p> <p>After successful connection, all traffic through your modem is routed by the ISP over the Internet to your PPTP server, which routes the traffic to the correct computer.</p> <p>Installing NT Page 24: You do not need to make a second dial-up call because the ISP server configured as a PPTP client, makes the connection to the PPTP server for the PPP client.</p>

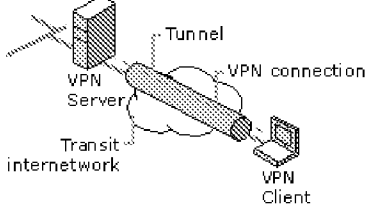
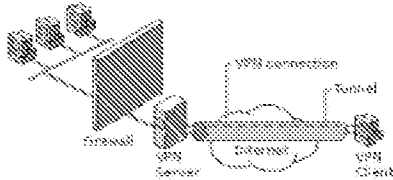
Appendix H
Citations to Exemplary Description in the Microsoft VPN*

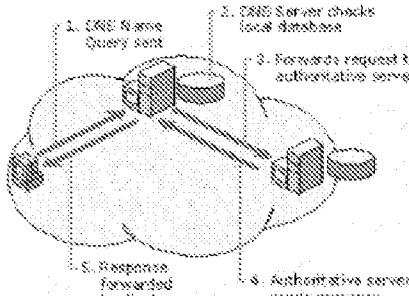
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
<p>1. A method for accessing a secure computer network address, comprising steps of:</p>	<p>Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server.</p> <p>Microsoft VPN, Page 13: For the VPN connection to be established, the VPN server authenticates the VPN client attempting the connection and verifies that the VPN client has the appropriate permissions. If mutual authentication is being used, the VPN client also authenticates the VPN server, providing protection against masquerading VPN servers.</p> <p>Microsoft VPN, Page 34:</p>  <p style="text-align: center;">Figure 13: VPN Server on the Internet in Front of the Firewall</p>
<p>receiving a secure domain name;</p>	<p>Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user name must match the name of a demand-dial interface on the corporate office VPN server.</p>
<p>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>Microsoft VPN, Page 66:</p>

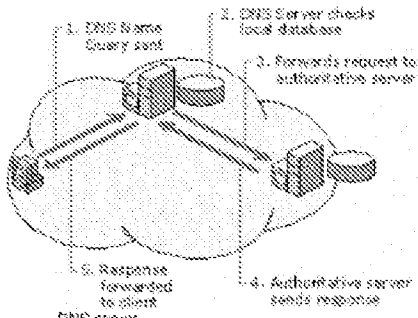
* - The cited passages are an indication of where in the Microsoft VPN reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

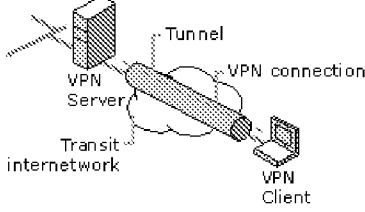
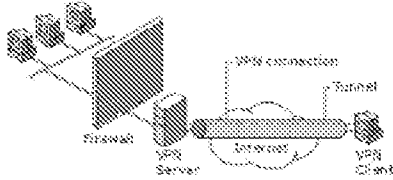
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the local database. 3. If the FQDN is not found, the DNS server forwards the request to an authoritative server. 4. The authoritative server sends the response. 5. The response is forwarded to the client.  <p>The diagram illustrates the DNS resolution process. A client (represented by a computer icon) sends a 'DNS Name Query' (labeled 1) to a 'DNS server' (represented by a server rack icon). The DNS server checks its 'local database' (labeled 2). If the query is not found, the DNS server forwards the request to an 'authoritative server' (represented by another server rack icon). The authoritative server sends a response (labeled 4) back to the DNS server. The DNS server then forwards the response (labeled 5) back to the client.</p> <ol style="list-style-type: none"> 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Microsoft VPN, Page 66:</p>

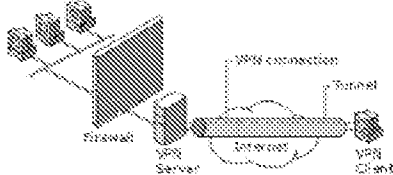
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to give a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. It shows a client (represented by a computer icon) sending a '1. DNS Name Query sent' to a 'DNS server'. The DNS server then '2. forwards request to authoritative server'. The authoritative server '4. authoritative server sends response' back to the original DNS server. Finally, the original DNS server '5. Response forwarded to client'.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . .</p> <p>A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.</p> <p>Microsoft VPN Page 12:</p>

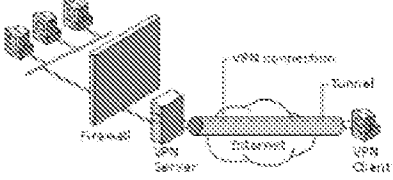
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	 <p>The diagram illustrates a VPN setup. On the left, a server icon is labeled 'VPN Server'. A line connects it to a cloud labeled 'Transit internetwork'. From the cloud, a line goes to a laptop icon labeled 'VPN Client'. A dashed line labeled 'Tunnel' connects the VPN Server and the VPN Client. A label 'VPN connection' points to the line between the Transit internetwork and the VPN Client.</p>
<p>10. The method according to claim 1, wherein the virtual private network includes the Internet.</p>	<p>Microsoft VPN, Page 34:</p>  <p>The diagram shows a sequence of components: a 'Firewall' icon, a 'VPN Server' icon, a cloud labeled 'Internet', and a 'VPN Client' icon. A line connects the Firewall to the VPN Server, then to the Internet, and finally to the VPN Client. A label 'VPN connection' points to the line between the VPN Server and the Internet.</p> <p>Figure 3.3: VPN Server not the located in Front of the Firewall</p>
<p>12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Microsoft VPN, Page 11: A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.</p> <p>... .</p> <p>VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet.</p>
<p>13. The method of claim 1, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer</p>	<p>Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user</p>

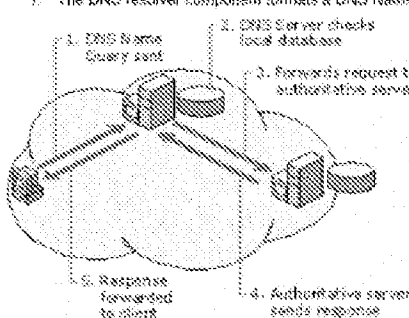
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
from a user;	name must match the name of a demand-dial interface on the corporate office VPN server.
<p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>Microsoft VPN, Page 66:</p> <p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. It shows a client computer on the left and a DNS server on the right. The client sends a '1. DNS Name Query sent' to the DNS server. The DNS server performs a '2. DNS Server checks local database'. If not found, it '3. Forwards request to authoritative server'. The authoritative server '4. Authoritative server sends response' back to the DNS server. Finally, the DNS server '5. Response Forwarded to client'.</p>
<p>wherein receiving the response message comprises receiving the response message at the client computer;</p>	Microsoft VPN, Page 66:

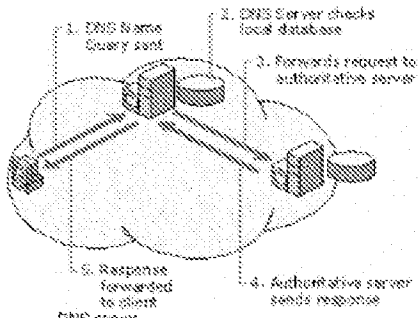
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. It shows a client (represented by a computer icon) sending a '1. DNS Name Query sent' to a 'DNS server'. The DNS server performs '2. DNS Server checks local database'. If not found, it '3. Forwards request to authoritative server'. The 'authoritative server' then '4. authoritative server sends response' back to the original DNS server. Finally, the original DNS server '5. Response forwarded to client'.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . .</p> <p>A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.</p> <p>Microsoft VPN Page 12:</p>

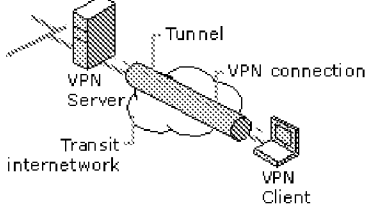
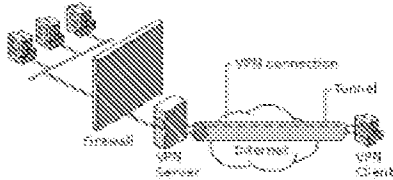
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	 <p>The diagram illustrates a VPN setup. On the left, a server icon is labeled 'VPN Server'. On the right, a laptop icon is labeled 'VPN Client'. A cloud-like shape between them is labeled 'Transit internetwork'. A thick, shaded line representing a 'Tunnel' connects the VPN Server and the VPN Client. A dashed line labeled 'VPN connection' also connects the two, passing through the transit internetwork.</p>
14. The method of claim 1, performed by a software module.	See claim 1, which is performed by Windows NT 4.0 at the client computer.
15. The method of claim 1, performed by a client computer.	See claim 1, which is performed by Windows NT 4.0 at the client computer.
17. A computer-readable storage medium, comprising:	<p>Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 34:</p>  <p>The diagram shows a network architecture. On the left, a server icon is labeled 'VPN Server'. To its right is a large rectangular block labeled 'Firewall'. On the far right, a laptop icon is labeled 'VPN Client'. A thick, shaded line representing a 'VPN connection' connects the VPN Server and the VPN Client. The connection passes through the Firewall. The area between the Firewall and the VPN Client is labeled 'Internet'.</p> <p>Figure 13: VPN Server on the Internet in Front of the Firewall</p>

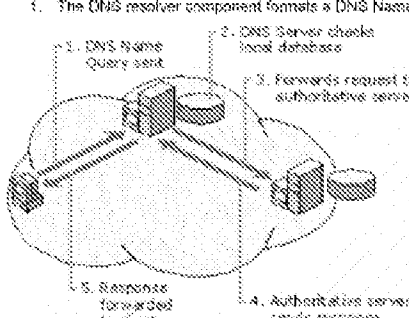
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
<p>a storage area; and</p>	<p>Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server.</p> <p>Microsoft VPN, Page 34:</p>  <p>Figure 13: VPN Server on the Internet in Front of the Firewall</p>
<p>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server.</p> <p>Microsoft VPN, Page 13: For the VPN connection to be established, the VPN server authenticates the VPN client attempting the connection and verifies that the VPN client has the appropriate permissions. If mutual authentication is being used, the VPN client also authenticates the VPN server, providing protection against masquerading VPN servers.</p> <p>Microsoft VPN, Page 34:</p>

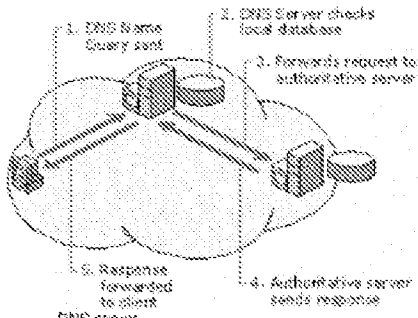
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	 <p data-bbox="524 804 881 835">Figure 1.2: VPN Server on the Internet in Front of the Firewall</p>
receiving a secure domain name;	Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user name must match the name of a demand-dial interface on the corporate office VPN server.
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	Microsoft VPN, Page 66:

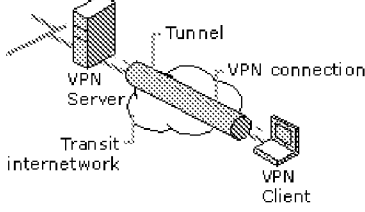
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the local database. 3. If the FQDN is not found, the DNS server forwards the request to an authoritative server. 4. The authoritative server sends the response back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. A client (represented by a computer icon) sends a 'DNS Name Query' (1) to a 'DNS server' (represented by a server rack icon). The DNS server checks its 'local database' (2). If the query is not found, the DNS server 'forwards request to authoritative server' (3). The 'authoritative server' (represented by another server rack icon) sends a 'response' (4) back to the original DNS server. Finally, the original DNS server sends the 'Response forwarded to client' (5) back to the client.</p> <ol style="list-style-type: none"> 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
<p>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Microsoft VPN, Page 66:</p>

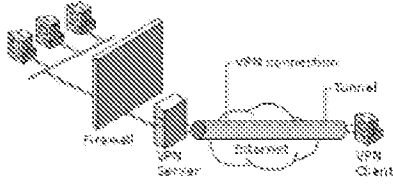
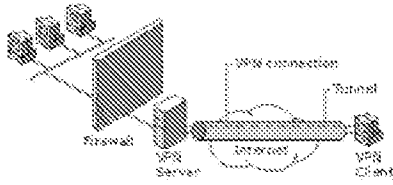
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to give a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. A client sends a 'DNS Name Query' (1) to a 'DNS server'. The DNS server checks its 'local database' (2). If the record is not found, it 'forwards request to authoritative server' (3). The 'authoritative server' sends a 'response' (4) back to the original DNS server. Finally, the original DNS server sends the 'Response forwarded to client' (5).</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . .</p> <p>A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.</p> <p>Microsoft VPN Page 12:</p>

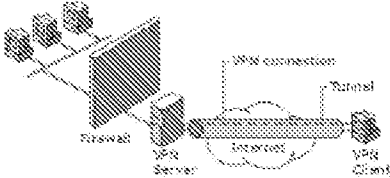
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	 <p>The diagram illustrates a VPN setup. On the left, a 'VPN Server' is shown. It is connected to a 'Transit internetwork' represented by a cloud. A 'Tunnel' is formed between the VPN Server and a 'VPN Client' on the right. The connection between the VPN Server and the VPN Client is labeled as a 'VPN connection'.</p>
<p>26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.</p>	<p>Microsoft VPN, Page 34:</p>  <p>The diagram shows a 'Firewall' on the left, connected to a 'VPN Server'. The VPN Server is connected to the 'Internet' (represented by a cloud). A 'VPN Client' is connected to the Internet. A 'VPN connection' is established between the VPN Server and the VPN Client. The VPN Server is positioned behind the Firewall.</p> <p>Figure 3.2: VPN Server not the located in Front of the Firewall</p>
<p>28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>Microsoft VPN, Page 11: A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.</p> <p>... .</p> <p>VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet.</p>
<p>29. The computer-readable medium according to claim 17,</p>	
<p>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer</p>	<p>Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user</p>

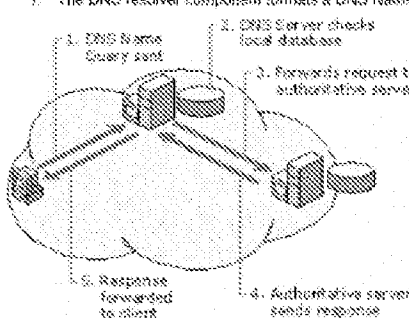
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
<p>from a user;</p> <p>wherein sending the query message comprises sending the query message at the client computer;</p>	<p>name must match the name of a demand-dial interface on the corporate office VPN server.</p> <p>Microsoft VPN, Page 66:</p> <p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is substantially simplified to gain a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured  <p>The diagram illustrates the DNS resolution process. A client (represented by a computer icon) sends a 'DNS Name Query' (labeled 1) to a 'DNS server' (represented by a server rack icon). The DNS server checks its 'local database' (labeled 2). If the record is not found, the DNS server 'forwards request to authoritative server' (labeled 3). The 'authoritative server' (represented by another server rack icon) returns a 'response' (labeled 4). The DNS server then 'forwards response to client' (labeled 5).</p> <ol style="list-style-type: none"> 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
<p>wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>Microsoft VPN, Page 66:</p>

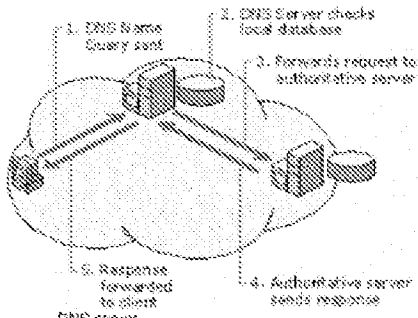
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to give a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. A client (represented by a computer icon) sends a '1. DNS Name Query sent' to a 'DNS server'. The DNS server performs '2. DNS Server checks local database'. If the record is not found, it performs '3. Forwards request to authoritative server' to an 'Authoritative server'. The authoritative server performs '4. Authoritative server sends response' back to the original DNS server. Finally, the original DNS server performs '5. Response forwarded to client' back to the client.</p>
<p>wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . .</p> <p>A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.</p> <p>Microsoft VPN Page 12:</p>

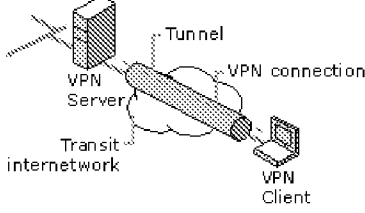
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	 <p>The diagram illustrates a Virtual Private Network (VPN) setup. On the left, a server icon is labeled 'VPN Server'. A cloud-like shape in the center is labeled 'Transit internetwork'. A thick, shaded line representing a 'Tunnel' connects the VPN Server to a laptop icon on the right labeled 'VPN Client'. A dashed line labeled 'VPN connection' also connects the VPN Server to the VPN Client, passing through the Transit internetwork.</p>
<p>30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.</p>	<p>See claim 1, which is performed by Windows NT 4.0 at the client computer.</p>
<p>31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.</p>	<p>See claim 1, which is performed by Windows NT 4.0 at the client computer.</p>
<p>33. A data processing apparatus, comprising:</p>	<p>Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 34:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	 <p data-bbox="521 800 881 835">Figure 12: VPN Server on the Internet in Front of the Firewall</p>
<p data-bbox="220 867 354 888">a processor, and</p>	<p data-bbox="516 867 1455 1052">Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 34:</p>  <p data-bbox="521 1276 881 1312">Figure 13: VPN Server on the Internet in Front of the Firewall</p>
<p data-bbox="144 1344 493 1482">memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p data-bbox="516 1344 1455 1505">Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server.</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>Microsoft VPN, Page 13: For the VPN connection to be established, the VPN server authenticates the VPN client attempting the connection and verifies that the VPN client has the appropriate permissions. If mutual authentication is being used, the VPN client also authenticates the VPN server, providing protection against masquerading VPN servers.</p> <p>Microsoft VPN, Page 34:</p>  <p>Figure 13: VPN Server on the Internet in Front of the Firewall</p>
receiving a secure domain name;	<p>Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user name must match the name of a demand-dial interface on the corporate office VPN server.</p>
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	<p>Microsoft VPN, Page 66:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. A client (represented by a computer icon) sends a 'DNS Name Query' (labeled 1) to a 'DNS server' (represented by a server rack icon). The DNS server checks its 'local database' (labeled 2). If the record is not found, the DNS server 'forwards request to authoritative server' (labeled 3). The 'authoritative server' (represented by another server rack icon) sends a 'response' (labeled 4) back to the original DNS server. The original DNS server then sends the 'Response forwarded to client' (labeled 5) back to the client.</p>
<p>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>Microsoft VPN, Page 66:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	<p>The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to give a basic understanding of the DNS resolution process.</p> <ol style="list-style-type: none"> 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server. 2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.  <p>The diagram illustrates the DNS resolution process. A client (represented by a computer icon) sends a '1. DNS Name Query sent' to a 'DNS server'. The DNS server performs '2. DNS Server checks local database'. If the record is not found, it '3. Forwards request to authoritative server'. The 'authoritative server' then '4. authoritative server sends response' back to the original DNS server. Finally, the original DNS server '5. Response forwarded to client'.</p>
<p>sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . .</p> <p>A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.</p> <p>Microsoft VPN Page 12:</p>

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	 <p>The diagram illustrates a VPN connection setup. On the left, a server icon is labeled 'VPN Server'. A cloud-like shape in the center is labeled 'Transit internetwork'. A thick, shaded cylinder representing a 'Tunnel' connects the VPN Server to a laptop icon on the right labeled 'VPN Client'. A dashed line labeled 'VPN connection' points to the tunnel. The entire setup is enclosed in a rectangular frame.</p>



Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Requester's Name and Address: WILLIAM N. HUGHET
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET, NW, SUITE 800
WASHINGTON, DC 20005

Patent Number: 7,188,180 Request Receipt Date: 11-25-2009

Control Number: 95/001,270
Date Mailed: 12-03-2009

NOTICE OF FAILURE TO COMPLY WITH *INTER PARTES* REEXAMINATION REQUEST FILING REQUIREMENTS (37 CFR 1.915(d))

The Central Reexamination Unit (CRU) in the United States Patent and Trademark Office (USPTO) has received a request for *inter partes* reexamination. The request cannot be processed, because the below-identified filing date requirements for an *inter partes* reexamination request have not been satisfied. If a fully compliant response is not received within 30 days of the mailing date of this notice, the request will be treated as a prior art citation under 37 CFR 1.501 or closed from public view, at the Office's option. A filing date will **NOT** be assigned to the request until the deficiencies noted below are corrected (37 CFR 1.919(a)).

The following items required by **37 CFR 1.915** are missing:

- 1. The *inter partes* reexamination filing fee under 37 CFR 1.20(c)(2) – see Attached Form PTO-2057.
- 2. An identification of the patent by its patent number, and of every claim of the patent for which reexamination is requested.
- 3. A citation of the patents and printed publications that are presented to raise a substantial new question of patentability.
- 4. A statement pointing out each substantial new question of patentability based on the cited patents & printed publications, and a detailed explanation of the pertinency and manner of applying the patents & printed publications to every claim for which reexamination is requested.
- 5. A legible copy of every patent or printed publication (other than U.S. patents or U.S. patent publications) relied upon or referred to in (3) and (4) above, accompanied by an English language translation of all the necessary and pertinent parts of any non-English language document.
- 6. A legible copy of the entire patent including the front face, drawings, and specification/claims (in **double** column format) for which reexamination is requested, and a copy of any disclaimer, certificate of correction, or reexamination certificate issued in the patent. All copies must have each page plainly written on only one side of a sheet of paper.
- 7. A certification by the third party requester that a copy of the request has been served in its entirety on the patent owner at the address provided for in 37 CFR 1.33(c). The name and address of the party served must be indicated. If service was not possible, a duplicate copy of the request must be supplied to the Office.
- 8. A certification by the third party requester that the estoppel provisions of 37 CFR 1.907 do not prohibit the *inter partes* reexamination.
- 9. A statement identifying the real party in interest to the extent necessary for a subsequent person filing an *inter partes* reexamination request to determine whether that person is a privity of the real party in interest.
- 10. Other item: See Attachment.
- Explanation of above item(s): See Attachment.

Any written correspondence in response to this notice must include a submission pursuant to the attached instructions. **The instructions for a detailed explanation for an *inter partes* reexamination request differ from those for an *ex parte* reexamination request.** Any written correspondence in response to this notice should be mailed to the Central Reexamination Unit (CRU), ATTN: "Box *Inter Partes* Reexam" at the USPTO address indicated at the top of this notice. Any "replacement documents" may be facsimile transmitted to the CRU at the FAX number indicated below. A REPLACEMENT STATEMENT AND EXPLANATION UNDER 37 CFR 1.915(b)(3) MAY NOT BE FACSIMILE TRANSMITTED.

Manuel Sullana

Patent Reexamination Specialist, Central Reexamination Unit
(571) 272-6825 ; FAX No. (571) 273-9900

cc: Patent Owner's Name and Address: BANNER & WITCOFF, LTD
1100 13TH STREET, NW
SUITE 1200
WASHINGTON, DC 20005-4051

ATTACHMENT TO PTOL-2076

Control Number: 95/001,270
Patent Number: 7,188,180
Request Receipt Date: 11/25/2009

A request for *inter partes* reexamination (or for *ex parte* reexamination) must now meet all the applicable statutory and regulatory requirements before a filing date is accorded to the request. See MPEP 2227 Part B.1 and MPEP 2217, Part I. See also *Clarification of Filing Date Requirements for Ex Parte and Inter Partes Reexamination Proceedings*, 71 Fed. Reg. 44219 (August 4, 2006), 1309 *Off. Gaz. Pat. Office* 216 (August 29, 2006) (final rule.)

The request submitted on November 25, 2009, cannot be processed because all of the filing date requirements for an *inter partes* reexamination have not been satisfied. The Request for Reexamination does not comply with the filing requirement of an *Inter Partes* reexamination proceeding under 37 CFR 1.915(b)(3), which requires “[a] statement pointing out each substantial new question of patentability based on the cited patents and printed publications, and a detailed explanation of the pertinency and manner of applying the patents and printed publications to every claim for which reexamination is requested.

Reexamination was requested for U.S. Patent No. 7,188,180 (in this instance claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33 and 35 are requested).

The request is incomplete as to compliance with 37 CFR 1.915(b)(3) for the following reason.

The request has failed to provide the requisite identification and explanation, in compliance with 37 CFR 1.915(b)(3), of what substantial new questions of patentability (SNQs) are being raised **by the cited prior art documents under 37 CFR 1.915(b)**. The request fails to clearly point out and explain how each asserted SNQ is substantially different from those raised in the previous examination of the patent before the Office. **It is not sufficient to merely state that the references were not of record in the prior prosecution of the ‘180 patent.** Also, as pointed out in MPEP 2616, “[i]t is not sufficient that a request for reexamination merely proposes one or more rejections of a patent claim or claims as a basis for reexamination. **It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching** that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during prosecution of any other prior proceeding involving the patent for which reexamination is requested.” [Emphasis added]

Under 35 U.S.C. 311, the requester must “set forth the pertinency and manner of applying cited prior art to every claim for which reexamination is requested.” Then, under 35 U.S.C. 312 and 313, the Office must determine whether “a substantial new question of patentability” affecting any claim of the patent has been raised by a request for reexamination.

To implement these statutory provisions, 37 CFR 1.915(b)(3) requires that the request include “a statement pointing out each substantial new question of patentability based on the cited patents and printed publications...” See MPEP 2617.

Accordingly, it is mandatory that the request clearly set forth in detail the specifics of what the third party requester considers the “substantial new question of patentability” to be. A request will point out how any questions of patentability raised are substantially different from those raised in the previous examination of the patent before the Office. See MPEP 2616.

If the requester were permitted to omit an explanation of how such documents cited in request are applied to the patent claims, an undue burden would be placed on the Office to address each document in the determination on the request, without an explanation of the relevance to the patent claims. Accordingly, such an omission is prohibited by law.

In view of the above discussion, the request does not provide a “statement pointing out each substantial new question of patentability based on the cited patents and printed publications, and a detailed explanation of the pertinency and manner of applying the patents and printed publications to every claim for which reexamination is requested,” as is required by 37 CFR 1.915(b)(3).

In accordance with 37 CFR 1.915(b), a filing date for the reexamination request will not be granted **at this time**.

Requester has the option to respond to this identification of a defect by using the appropriate option(s) set forth below:

1. A replacement statement and explanation pursuant to 37 CFR 1.915(b)(3), as detailed in the attached instructions. A statement identifying a substantial new question of patentability and an accompanying explanation must be provided for **EACH** of the documents that the requester desires the Office to consider.
2. Requester may either submit an explanation of the pertinency and manner of applying each of the cited prior art documents for every claim for which reexamination is requested in accordance with 37 CFR 1.915(b)(3).
3. A replacement Form PTO/SB/08a PTO-1449, or equivalent listing **ONLY** those references (with proper page designation, where appropriate) discussed in a proposed rejection (or statement identifying a substantial new question) and in a corresponding explanation under 37 CFR 1.915(b)(3).

Failure to submit a proper response to this Notice may result in the termination of the request, with no filing date accorded.

All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at <https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html>.

By Mail to: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

INSTRUCTIONS TO NOTICE OF FAILURE TO COMPLY WITH *INTER PARTES* REEXAMINATION REQUEST FILING REQUIREMENTS (37 CFR 1.915)

HOW TO REPLY TO THIS NOTICE

Any written correspondence in response to this notice must include either a replacement document, or, if item #4 is checked and/or it is otherwise specifically required by the Office, a paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3) that either replaces the originally-filed statement and explanation or provides a previously missing statement and explanation. A replacement document either replaces an originally-filed document, or provides a previously missing document, that contains part(s) of the request other than the statement and explanation as set forth in 37 CFR 1.915(b)(3). For example, a replacement to the originally-filed listing of cited patents and printed publications, PTO/SB/08 (formerly designated as PTO-1449) or its equivalent, is a replacement document.

If a paper containing a replacement statement and explanation, or a replacement document (other than a replacement certificate of service), is submitted by a third party requester, it must be accompanied by a certification that a copy of the replacement statement and explanation under 37 CFR 1.915(b)(3), or that a copy of the replacement document, has been served in its entirety on the patent owner at the address provided for in 37 CFR 1.33(c). The name and address of the party served must be indicated. If service was not possible, a duplicate copy of the replacement statement and explanation (or replacement document) must be supplied to the Office.

REPLACEMENT STATEMENT AND EXPLANATION UNDER 37 CFR 1.915(b)(3) (ITEM #4 IS CHECKED)

The statement and explanation under 37 CFR 1.915(b)(3) (see item #4) must discuss EVERY patent or printed publication cited in the information disclosure statement in at least one proposed rejection or statement identifying a substantial new question of patentability (SNQ), AND in a corresponding detailed explanation (see the below discussion). Furthermore, EVERY claim for which reexamination is requested must be discussed in at least one proposed rejection or statement identifying an SNQ and in the corresponding detailed explanation. If item #4 is missing or incomplete, a paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3) is required.

A paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3) may NOT be facsimile transmitted. It must be received by first class mail or by U.S. Postal Service (USPS) Express Mail.

If an originally-filed information disclosure statement cites patents or printed publications that are NOT discussed in at least one proposed rejection or statement identifying an SNQ AND in the corresponding detailed explanation in the originally-filed request, then the requester must file either (a) a replacement document, i.e., a replacement PTO/SB/08 (former PTO-1449) or its equivalent, listing ONLY those patents and printed publications that are so discussed, or (b) a paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3). If the first option is chosen, the replacement PTO/SB/08 or its equivalent should include a cover letter expressly withdrawing from the request any previously cited references that are being omitted by the replacement PTO/SB/08 or its equivalent. The requester may, if desired, file both a replacement PTO/SB/08 or its equivalent and a paper containing a replacement statement and explanation, if the replacement statement and explanation discusses EVERY patent or printed publication, cited in the replacement PTO/SB/08 or its equivalent, in at least one proposed rejection or statement identifying an SNQ and in the corresponding detailed explanation.

Requester is NOT required to, and should not, additionally file a replacement copy of any exhibits, references, etc., or other replacement parts of the request (i.e., replacement documents) if a defect requiring a replacement document is not specifically identified by this notice.

Examples of When a Replacement Statement and Explanation under 37 CFR 1.915(b)(3) Is Required:

1. The originally-filed request fails to discuss EVERY patent or printed publication cited in the originally-filed information disclosure statement in at least one proposed rejection or statement identifying an SNQ and in the corresponding detailed explanation, and the requester does not wish to file a replacement PTO/SB/08 (formerly designated as PTO-1449) or its equivalent listing ONLY those patents and printed publications that are so discussed.
2. The originally-filed request discusses every patent or printed publication cited in the information disclosure statement in at least one proposed rejection or statement identifying an SNQ, but fails to discuss EVERY patent or printed publication cited in the information disclosure statement in a detailed explanation that corresponds to the proposed rejection or statement identifying an SNQ.
3. The originally-filed request fails to discuss EVERY CLAIM for which reexamination is requested in at least one proposed rejection or statement identifying an SNQ, and in the corresponding detailed explanation.

Examples of Proposed Rejections and Statements Identifying a Substantial New Question of Patentability (SNQ)**Proposed rejections**

Claims 1-3 are obvious over reference A in view of reference B.
Claims 4-6 are obvious over reference A in view of references B and C.
Claims 7-10 are obvious over reference Q in view of reference R.

Statements identifying a substantial new question of patentability

A substantial new question of patentability as to claims 1-3 is raised by reference A in view of reference B.
A substantial new question of patentability as to claims 4-6 is raised by reference A in view of references B and C.
A substantial new question of patentability as to claims 7-10 is raised by reference Q in view of reference R.

A proposed rejection or statement identifying an SNQ must be repeated with any *replacement* detailed explanation that corresponds to the proposed rejection or statement identifying an SNQ, in any paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3).

In addition, the requester should include an explanation of *how the SNQ is raised*.

1. Assume that claim 1 of the patent recites, as one of the limitations, widget W. Requester would state that the XYZ reference, cited in the information disclosure statement, contains a teaching of widget W as recited in claim 1, and that this teaching was not present during the prior examination of the patent under reexamination (i.e., the teaching is "new"). Requester would also state that he believes that a reasonable examiner would consider this teaching important in determining whether or not the claims are patentable. For this reason, requester would state that this teaching by the XYZ reference raises a substantial new question of patentability (SNQ) with respect to at least claim 1 of the patent. Similarly, if dependent claim 6 adds widget H, the requester would state that the ABC reference, cited in the information disclosure statement, contains a teaching of widget H as recited in claim 6, that this teaching was not present during the prior examination of the patent, that a reasonable examiner would consider this teaching important in determining whether or not the claims are patentable, and that this teaching raises an SNQ with respect to dependent claim 6 of the patent.

2. Assume that claim 1 of the patent recites, as one of its limitations, limitation W. Assume either that reference XYZ was applied in a rejection during the prior examination of the patent, or that the teachings of reference XYZ are purely cumulative to a reference cited in a rejection during the prior examination of the patent. Assume further that reference ABC teaches that the limitation W would have been either inherent given the teachings of reference XYZ, or would have been obvious in view of the combination of XYZ and ABC. Reference ABC was cited in an information disclosure statement but was never discussed or applied in a rejection ***in combination with the XYZ reference*** during the prior examination of the patent under reexamination. **Requester would state that reference XYZ was present during the prior examination of the patent under reexamination because it was applied in a rejection during the prosecution of the patent, and that reference ABC was cited in an information disclosure statement but never applied in a rejection (or never discussed), ***in combination with the XYZ reference*** during the prior examination of the patent under reexamination.** Requester would then state (1) that the ***combination*** of the XYZ reference and the ABC reference, both of which are cited in the information disclosure statement, contains a teaching of limitation W as recited in claim 1, (2) that this teaching provided by the ***combination*** of the XYZ and ABC references was not presented during the prior examination of the patent under reexamination, (3) that a reasonable examiner would consider this teaching important in determining whether or not the claims are patentable, and (4) that the presentation of this teaching raises a SNQ with respect to claim 1 of the patent.

Example of a Detailed Explanation

Assume, for example, that a requester believes that the XYZ reference, alone, anticipates claims 1-5. The requester would expressly propose a rejection of claims 1-5 under 35 USC 102(b) as being anticipated by the XYZ reference. In a claim chart, the requester would then show how each limitation of claims 1-5 is anticipated by the XYZ reference. If the requester believes that the XYZ reference, in view of the ABC reference, renders obvious claims 6-10, the requester would expressly propose a rejection of claims 6-10 under 35 USC 103 as being obvious over the XYZ reference in view of the ABC reference. In a claim chart, the requester would then show which limitations of claims 6-10 are taught by the XYZ reference, and which limitations of claims 6-10 are taught by the ABC reference. The requester should quote each pertinent teaching in the prior art reference, referencing each quote by page, column and line number, and any relevant figure numbers. Finally, for a proposed rejection, the requester must show how these two references are combined, and the teaching in either the XYZ or the ABC references which provides the motivation to combine these references in order to render claims 6-10 obvious.

REPLACEMENT DOCUMENTS

If the originally-filed PTO/SB/08 (former PTO-1449) or its equivalent lists patents or printed publications that are NOT discussed in at least one proposed rejection or statement identifying an SNQ AND in the corresponding detailed explanation in the originally-filed request, the requester may file a paper containing a replacement PTO/SB/08 (former PTO-1449) or its equivalent listing ONLY those patents and printed publications that are so discussed. The replacement PTO/SB/08 or its equivalent should include a cover letter expressly withdrawing from the request any previously cited references that are now being omitted by the replacement PTO/SB/08 or its equivalent. Similarly, if any patent or printed publication discussed in at least one proposed rejection or statement identifying an SNQ AND in the corresponding detailed explanation in the originally-filed request is not listed in the originally-filed PTO/SB/08 (former PTO-1449) or its equivalent, the requester must file a replacement PTO/SB/08 (former PTO-1449) or its equivalent listing all of the patents and printed publications, including the previously omitted reference(s), and provide copies of the missing references if copies were not provided with the originally-filed request.

If a copy of a patent, printed publication, or an English-language translation of a patent or printed publication, that is cited in the PTO/SB/08 (former PTO-1449) or its equivalent, is illegible, missing, or incomplete (i.e., it does not contain all of the pages indicated in the PTO/SB/08 (former PTO-1449) or its equivalent), a replacement copy of the patent or printed publication is required.

If a copy of any disclaimer, certificate of correction, or reexamination certificate issued in the patent, or a copy of the entire patent for which reexamination is requested as described in item #6, is missing, or if the copy that was received by the Office was illegible or incomplete, a replacement document (i.e., a replacement copy of the disclaimer, certificate of correction, reexamination certificate, or entire patent under reexamination as described in item #6) is required.

If the requester fails to correctly identify the patent number or the claims for which reexamination is requested on the transmittal form for the request (PTO/SB/57, or an equivalent) as described in item #2, and the patent number and the claims for which reexamination is requested are correctly identified in the originally-filed request, a replacement transmittal form is required.

If a certificate of service on the patent owner, as described in item #7, is missing, or if the certificate of service received by the Office is inaccurate or incomplete, a replacement certificate of service is required.

Replacement documents may be facsimile transmitted. A paper containing a replacement statement and explanation may NOT be facsimile transmitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No: 7,188,180)	
)	
Victor LARSON, et al.)	Reexam Control
)	No. 95/001,270
Issued: March 6, 2007)	
)	
Filed: November 7, 2003)	
)	
Title: METHOD FOR ESTABLISHING)	
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF VIRTUAL)	
PRIVATE NETWORK)	

REPLACEMENT REQUEST FOR *INTER PARTES* REEXAMINATION OF PATENT

Attn: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Replacement Request for *Inter Partes* Reexamination is being filed in response the Notice of Failure to Comply with *Inter Partes* Reexamination Request Filing Requirements, dated December 3, 2009, objecting to the prior Request for *Inter Partes* Reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of U.S. Patent No. 7,188,180. The present reexamination request corrects the deficiencies of the November 25, 2009 request by expressly pointing out each substantial new question of patentability and providing a detailed explanation of the pertinency and manner of applying the printed publications to every claim for which reexamination is requested.

Reexamination is requested of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of U.S. Patent No. 7,188,180 (“the ‘180 patent”) to Larson et al., pursuant to 35 U.S.C. §§ 311 - 316 and 37 C.F.R. § 1.902 *et seq.* The ‘180 patent is entitled “Method for Establishing Secure

Communication Link Between Computers of Virtual Private Network” and issued March 6, 2007, from U.S. Patent Application No. 10/702,486, filed November 7, 2003. The requestor is Microsoft Corporation, and the ‘180 patent has not been previously reexamined.

Request for *Inter Partes* Reexamination

Requestor respectfully submits that there are substantial new questions regarding the patentability of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the ‘180 patent. These substantial new questions of patentability are based on previously uncited, and thus unconsidered, prior art references that render each of these claims unpatentable. Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the ‘180 patent are unpatentable in view of these new prior art references under 35 U.S.C. § 102 or 35 U.S.C. § 103. Accordingly, Requestor respectfully requests that this Request for Inter Partes Reexamination be granted. This Request for Inter Partes Reexamination satisfies the requirements of 37 C.F.R. § 1.915(b)(1) through (8) as follows:

37 C.F.R. § 1.915(b)(1): Reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of U.S. Patent No. 7,188,180 to Larson, et al. is requested.

37 C.F.R. § 1.915(b)(2): This reexamination request is based on the prior art references listed in Section III.

37 C.F.R. § 1.915(b)(3): A statement of each substantial new question of patentability is presented in Section II. A detailed explanation of the pertinency and manner of applying the prior art to each claim element in the requested claims is provided in Section V, based on the claim charts presented as Appendices A - H.

37 C.F.R. § 1.915(b)(4): Copies of the references relied upon in paragraphs (b)(1) through (3) above are submitted herein as Exhibits 2 - 11. The references relied upon are listed in an equivalent of a PTO Form 1449, which is submitted herewith as Exhibit 12.

37 C.F.R. § 1.915(b)(5): A copy of the entire ‘180 patent is submitted as Exhibit 1.

37 C.F.R. § 1.915(b)(6): Requester certifies this entire replacement reexamination request was served in its entirety on the purported patent owner at:

VirnetX, Inc.
c/o Banner & Witcoff, Ltd.
1100 13th Street, N.W., Suite 1200

Washington, D.C. 20005-4051

and

VirnetX, Inc.
5615 Scotts Valley Drive, Suite 110
Scotts Valley, Ca 95066

on the 8th day of December, 2009.

37 C.F.R. § 1.915(b)(7): Requestor certifies that this is a new reexamination request, and that therefore the estoppel provisions of 37 C.F.R. § 1.907 do not prohibit this Request.

37 C.F.R. § 1.915(b)(8): The real party in interest for this request is Microsoft Corporation.

As noted above, this request for *Inter Partes* Reexamination was initially filed November 25, 2009, and authorization to charge our Deposit Account No. 02-2135 in the amount of \$8,800.00 was submitted on that date, pursuant to 37 C.F.R. § 1.20(c)(2), to cover the fee of the Request for *Inter Partes* Reexamination. Accordingly, it is believed that no further fee is due at this time for submitting this replacement request. However, if any fee is required in connection with this resubmission, please charge our Deposit Account No. 02-2135.

Notification of Concurrent Proceedings

Pursuant to 37 C.F.R. § 1.985, Requestor provides notice that the ‘180 Larson patent is presently involved in a patent infringement action brought in the United States District Court for the Eastern District of Texas, the action having been assigned Case No. 6:07-cv-00080-LED and captioned “VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION VS. MICROSOFT CORPORATION.” (“the VirnetX case”). Microsoft Corporation is the Requestor of the present Request for Inter Partes Reexamination and, upon information and belief, VirnetX, Inc. is the alleged assignee of the ‘180 Larson patent.

The Requestor also provides notice that two additional patents in the family of the ‘180 patent are involved in the above-noticed VirnetX litigation, namely U.S. Patent Nos. 6,502,135 to Munger, et al. and 6,839,759 to Larson, et al. The Requestor is also filing herewith a separate Request for Inter Partes Reexamination of the 6,502,135 Munger et al. patent.

Disclaimer Regarding Claim Construction

In reexamination, the Patent Office must afford the claims the broadest reasonable interpretation consistent with the specification. *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984). The legal standards for claim construction in reexamination do not necessarily correspond to the legal standards that are mandated to be used by the courts in litigation. See MPEP §2686.05 (determination of a substantial new question of patentability is made independently of a court's decision on validity because the District Courts and the Patent Office use different standards of proof and claim interpretation); see also *In re Zletz*, 893 F.2d 319, 321, 13 USPQ2d 1320,1321-22 (Fed. Cir. 1989) (during patent examination, the pending claims must be interpreted as broadly as their terms reasonably allow). Requester submits that claim constructions discussed herein for the purposes of demonstrating a substantial new question of patentability are not binding upon Requester in any litigation.

I. Claims for Which Reexamination is Requested

Reexamination is respectfully requested for claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent under 35 U.S.C. §§ 311 - 316 and 37 C.F.R. § 1.902 *et seq.* Claims 1, 17, and 33 are independent claims. Claims 4, 10, and 12-15 depend, directly or ultimately, from independent claim 1; claims 20, 26, and 28-31 depend, directly or ultimately, from independent claim 17; and claim 35 depends directly from independent claim 33.

II. Substantial New Questions of Patentability

The Requestor respectfully submits that there are substantial new questions ("SNQ") regarding the patentability of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent. Each of these substantial new questions of patentability is based on prior art not cited during prosecution of the '180 patent and which render each of these claims unpatentable. Each of issued claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent are unpatentable in view of these prior art references under 35 U.S.C. § 102 and/or 35 U.S.C. § 103.

On November 21, 2006, a Notice of Allowance and a Notice of Allowability were mailed in the '180 patent application, wherein the Examiner asserted his statement of reasons for allowance:

The prior arts of record do not teach a system and a method for accessing a secure

computer network address comprising steps of: requesting a secure computer network address from a secure domain name server according to the secure domain name; and using a virtual private network communication link to send an access request message to the secure computer network address.

See Exhibit 14, Notice of Allowance. The statement of reasons for allowance is a paraphrase of independent claim 1 and includes many of the elements of independent claims 17 and 33, of which reexamination is being requested herein. Substantial new questions of patentability are raised because none of the references cited herein were considered by the Examiner during prosecution of the '180 patent application and because these references disclose, separately or in combination, teachings that are different from the prior art of record, and therefore new to the Examiner, that anticipate or render obvious each of the claimed elements that had been asserted by the Examiner to be the reason the claims were allowed. A reasonable Examiner would have found the teachings of these non-cumulative new references important in deciding whether the claims were patentable because the new references disclose the claimed elements that the Examiner believed were missing from the prior art of record, upon which basis the pending '180 patent application claims were allowed. The anticipatory and obviousness teachings of these new prior art references would have been found particularly important to a reasonable Examiner in view of the fact that no art rejection had ever been made during prosecution of the '180 patent application.

III. U.S. Patents and Printed References Which Raise a Substantial New Question of Patentability

Reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent is requested in view of the following references:

Exhibit 2. Aventail Administrator's Guide (hereafter "Aventail"), published in 1996 - 1999, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Aventail was not considered during prosecution of the '180 patent.

Exhibit 3. Microsoft, Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview"), published in 1998, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). VPN Overview was not considered during prosecution of the '180 patent.

- Exhibit 4. RFC 1035, published in 1987, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). RFC 1035 was not considered during prosecution of the '180 patent.
- Exhibit 5. David Kosiur, Building and Managing Virtual Private Networks (hereafter "Kosiur"), published in 1998, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Kosiur was not considered during prosecution of the '180 patent.
- Exhibit 6. Elizabeth Kaufman, Implementing IPsec (hereafter "Kaufman"), published in September 7, 1999, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Kaufman was not considered during prosecution of the '180 patent.
- Exhibit 7. James Galvin, Public Key Distribution with Secure DNS (hereafter "Galvin"), published in July 1996, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Galvin was not considered during prosecution of the '180 patent.
- Exhibit 8. Gauntlet Firewall for Windows NT, Administrator's Guide (hereafter "Gauntlet"), published no later than 1999, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Gauntlet was not considered during prosecution of the '180 patent.
- Exhibit 9. Microsoft Windows NT Technical Support: Hands-On, Self-Paced Training for Support Version 4.0 (hereafter "Hands-On"), published in 1998, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Hands-On was not considered during prosecution of the '180 patent.
- Exhibit 10. Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers (hereafter "Installing NT"), published in 1997, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Installing NT was not considered during prosecution of the '180 patent.
- Exhibit 11. Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources (hereafter "Microsoft VPN"), published in January 1, 2000, before the filing of the

'180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Microsoft VPN was not considered during prosecution of the '180 patent.

These new prior art references are non-cumulative to the prior art considered during the original prosecution of the '180 patent and raise substantial new questions of patentability with respect to at least claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 because they each teach, separately or in combination, the very claimed elements that the Examiner believed were absent in the prior art of record. The detailed explanation of the pertinency and application of the references to the claims is presented in Section V (identified by SNQ and page number in the table below). For each reference, there is an explanation of why it creates a substantial new question of patentability, either alone or in combination with other references, with respect to the claims of the '180 patent. The supporting claim charts illustrating the prior art disclosure from the references can be found in Appendices A-H.

Principal Reference	Substantial New Questions of Patentability Raised Alone Or In Combination With Other References	SNQ #	Page #	Claim Chart
Aventail Administrators Guide	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Aventail.	SNQ #1	12	Appendix A
VPN Overview	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103(a) for being obvious over VPN Overview in view of RFC 1035.	SNQ #2	19	Appendix B
Kosiur	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(b) for being anticipated by Kosiur.	SNQ #3	25	Appendix C
Kaufman	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Kaufman.	SNQ #4	30	Appendix D
Kaufman	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103 for being obvious over Kaufman in view of Galvin.	SNQ #5	36	Appendix E
Gauntlet	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Gauntlet.	SNQ #6	40	Appendix F
Hands On	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103(a) for being obvious over Hands On in view of Installing NT.	SNQ #7	45	Appendix G

Microsoft VPN	Claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Microsoft VPN.	SNQ #8	52	Appendix H
---------------	----------------------------------------------------------------------------------------------------------------------------------	--------	----	------------

IV. Overview of the ‘180 Patent, for Which Reexamination is Requested

A. Summary of the Disclosure & the Priority Date of the Claims of the ‘180 Patent

The ‘180 patent issued March 6, 2007 from U.S. Patent Application No. 10/702,486 (“the ‘486 application”), which was filed November 7, 2003. The ‘486 application is a divisional application of U.S. Patent Application No. 09/558,209, filed April 26, 2000, now abandoned (“the ‘209 application”). The ‘209 application is a continuation-in-part (“CIP”) application of U.S. Patent Application No. 09/504,783, filed February 15, 2000, now U.S. Patent No. 6,502,135 (“the ‘135 patent”). The ‘135 patent is a CIP application of U.S. Patent Application No. 09/429,643, filed October 29, 1999, now U.S. Patent No. 7,010,604 (“the ‘604 patent”). The ‘604 patent attempts to claim priority from Provisional Application No. 60/137,704, filed June 7, 1999, and Provisional Application No. 60/106,261, filed October 30, 1998. However, the effective filing date for the embodiments claimed in claims 1 - 41 of the ‘180 patent is no earlier than April 26, 2000, as explained below.

The ‘180 patent recites subject matter directed to a method for accessing a secure network address via a secure domain name service, the independent claims are styled as a method, a computer-readable storage medium (comprising instructions for a method for accessing a secure computer network), and a data processing apparatus (which include a memory storing instructions for a method for accessing a secure computer network address). The methodology recited in all three of the independent claims include the steps of receiving a secure domain name, sending a query message, receiving a response message, and sending an message requesting access to the secure network address. For example, independent claim 1 recites:

1. A method for accessing a secure computer network address, comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using

a virtual private network communication link.

independent claim 17 recites:

17. A computer-readable storage medium, comprising:
 - a storage area; and
 - computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.

and independent claim 33 recites:

33. A data processing apparatus, comprising:
 - a processor, and
 - memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.

To the extent there is allegedly any written description support, such written descriptive support for this claimed subject matter first appeared in the '209 CIP application, which was filed April 26, 2000, and of which the '180 is a continuation and shares the same specification, including the figures. For example, see the '180 patent at Col. 6, lines 27 - 33, where the '486 application discloses:

The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure

virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet.

The same disclosure can be found in the originally-filed specification of the '209 parent application at page 10, lines 22 - 26. Col. 7, lines 31 - 39 of the '486 application and page 11, lines 16 - 22 of the '209 application disclose:

The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network.

These portions of the Summary of the Invention were added with the April 26, 2000 filing of the '209 application. Similarly, new material was added on April 26, 2000, beginning at Col. 49, line 54 of the '486 application and page 81, line 15 of the '209 application, where the heading "One-Click Secure On-line Communications and Secure Domain Name Service" first appears.

Further in the '486 and '209 applications, there are disclosed the steps of "querying a secure domain name service" ('486 at Col. 51, line 34 and '209 at page 84, line 8), "Returning to FIG. 34, in step 3410, SDNS 3313 returns a secure URL to software module 3309 for the 'scom address for secure server 3320 corresponding to server 3304" ('486 at Col. 52, lines 38 - 40 and '209 at page 86, lines 1 - 3), and "At step 3411, software module 3309 accesses secure server 3320 through VPN communication link 3321 based on the VPN resources allocated by VPN gatekeeper 3314" ('486 at Col. 52, lines 55 - 57 and '209 at page 86, lines 14 - 16).

None of the four earlier filed applications from which priority is claimed by the '209 parent application includes these exemplary descriptions. Nor is there any other description in the four earlier applications for the claimed subject matter of the '180 patent. Accordingly, prior art as regards independent claims 1, 17, and 33 and, by dependency, claims 4, 10, 12-15, 20, 26, 28-31, and 35 would be any and all documents published before April 26, 2000, and patents with an effective filing date before April 26, 2000.

B. Prosecution History

Claims directed to the approximate or similar subject matter of issued claims 1 - 41 of the '180 patent were first filed on April 26, 2000 as claims 31 - 52 (claim 41 was omitted in the '209 application, and two claim 42's were filed) in the '209 parent application. Similarities can be found between issued '180 patent claims 1 and 17 and claim 31 and the second claim 42, respectively, of the '209 patent. Following a July 3, 2003 restriction requirement in the '209 parent application and an August 4, 2003 election by the Applicants of the '209 application, only claims 1 - 30 remained pending in the '209 application. A Notice of Allowance and a Notice of Allowability were mailed August 12, 2003, with no art rejection having been made by the Examiner. The issue fee for the '209 application was not paid, and a Notice of Abandonment was mailed December 23, 2003.

The '486 application was filed November 7, 2003, as a divisional of the '209 application, with the claims 1 - 24. Originally filed claims 1 - 22 of the '486 application matched claims 31 - 52 of the '209 application. A first Office Action was mailed May 19, 2006 in the '486 application, rejecting independent claims 1 and 12 under 35 U.S.C. § 112, second paragraph, and objecting to claims 2 - 11 and 13 - 24 as depending from a rejected base claim. An amendment in the '486 application was filed August 17, 2006, amending independent claims 1 and 12 by adding "from the secure domain name service" to the sending and the second receiving steps, and adding claims 25 - 41. A Notice of Allowance and a Notice of Allowability were mailed November 21, 2006, allowing all pending claims 1 - 41. No art rejection was ever made in the application. The Notice of Allowability included an Examiner's Statement of Reasons for Allowance:

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

The issue fee was paid January 16, 2007, and the '486 application proceeded to issue.

V. Explanation of the Pertinency and Manner of Applying Newly Cited Prior Art to Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 Patent, for Which Reexamination is Requested

SNQ #1 Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 102 (a) for being anticipated by Aventail

1. Substantial New Question of Patentability

Aventail's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Aventail teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Aventail discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Aventail discusses methods and systems for establishing a virtual private network ("VPN") across a network such as the Internet. Specifically, the reference discloses three main methods for creating a VPN according to Aventail: (1) a basic embodiment where the VPN determination is made at the client computer (p. 8), (2) a proxy chaining embodiment where the VPN determination is made at a proxy server (pp. 68, 72), and (3) a multiproxy embodiment where the VPN determination is made at both the client computer and successive proxy servers (pp. 68-71).

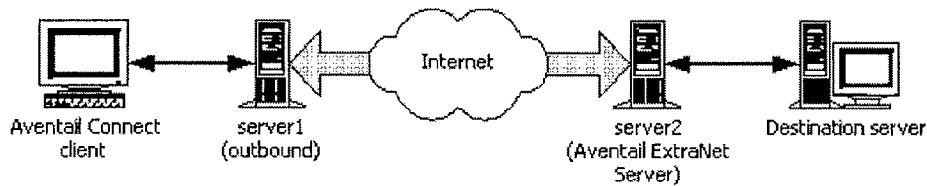
In the basic method, the process begins with the client computer requesting a domain name service (DNS) lookup of a hostname. (p. 8). Aventail Connect, a software program, intercepts the lookup request and determines whether the hostname corresponds to an entry in a list of hostnames maintained by Aventail Connect. If it does not correspond to an entry in the list, Aventail Connect permits the lookup to proceed as if Aventail Connection were not there –

i.e., a typical DNS resolution process. (p. 8). If the hostname is on the list, Aventail Connect recognizes that the hostname requires a VPN and initiates the VPN process according to Aventail. (p. 12). The entire process is transparent to the user, and the VPN according to Aventail is set up automatically based on the DNS lookup request issued by the client computer. (p. 12-13).

In the proxy chaining method, the functionalities of Aventail Connect are moved to a proxy server (p. 68 – “where one Aventail Extranet server acts as a client to another Aventail Extranet Server”). In other words, when the client computer requests a DNS lookup, the proxy server intercepts the lookup request and makes the determination whether the request is for a destination requiring a VPN connection according to Aventail.

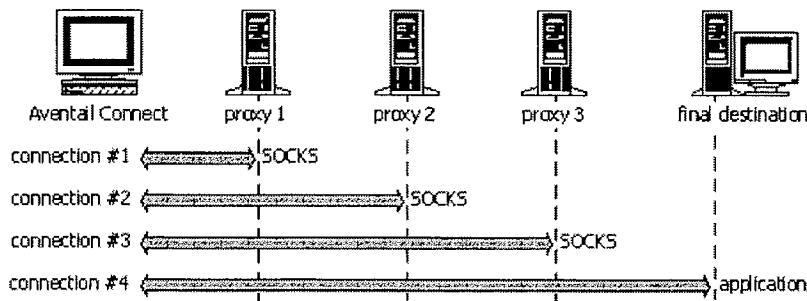
Aventail Connect 3.1/2.6 Admin Guide Page 72:

PROXY CHAINING: Server1 appears as a user to server2.



In the multiproxy method, Aventail Connect at the client computer makes an initial determination that a VPN according to Aventail is required in the same manner as the basic method. Where the process differs, however, is that Aventail Connect must negotiate with successive proxy servers to establish the VPN. (p. 69). Each successive proxy server has its own access and control rules for passing Aventail Client onto the next proxy server. (p. 68).

Aventail Connect 3.1/2.6 Admin Guide Page 69:



In each method, the entire process is transparent to the user and the VPN according Aventail is set up automatically. (p. 12-13).

3. Application of the Prior Art

Independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link. In particular, claim 1 recites:

1. A method for accessing a secure computer network address, comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.

Each of the steps of claim 1 is disclosed in the Aventail Administrator's Guide, which published no later than 1999, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application filing. As such, the 1999 Aventail Administrator's Guide is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Aventail is attached hereto as Appendix A.

The preamble of claim 1 requires "a method for accessing a secure computer network address." Aventail discloses such a feature at pages 46 and 79. Aventail creates SOCKS 5 connections for authenticated firewall traversal. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. Aventail at pages 12 and 46 discloses that authentication may be required

before access is granted to resources at the remote service.

Throughout this Request, Requester will reference the Court's July 30, 2009 claim constructions, included herein as Exhibit 13. This is not an admission that Requester agrees with the Court's constructions. The Requester is simply illustrating that the prior art references, even under the Court's constructions, anticipate and/or render obvious the claims of the '180 patent.

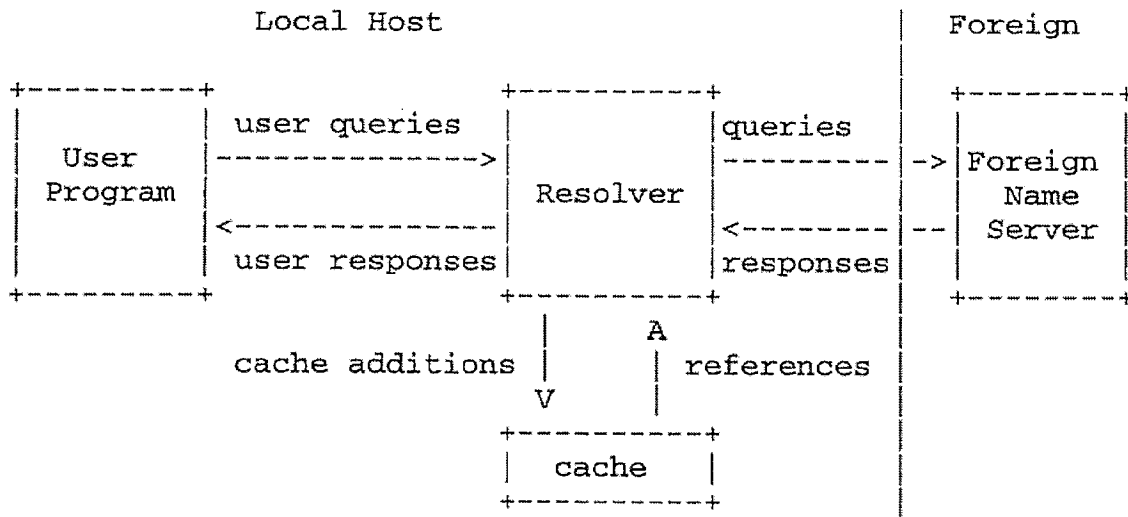
Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. Aventail discloses a domain name service for resolving domain names to IP addresses. See pages 11 and 12. Aventail Connect (the software at the client computer) receives a domain name from the user. The domain name is a secure domain name because it corresponds to a computer with an Aventail VPN connection that requires authentication before it can be accessed.

Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 12 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

There are two "lookup services" described in Aventail that independently satisfy this limitation. The first "lookup service" is a lookup service at the client computer. See page 8, which discusses a local DNS lookup. The alternative "lookup service" disclosed in Aventail is a more traditional DNS server that is located away from the client. See page 12, where the domain name is sent to the SOCKS server for resolution. In both cases, the domain name services are secure domain name services because they resolve the secure domain name to a corresponding secure computer network address.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." As discussed above, there are two "lookup services" disclosed in Aventail that independently satisfy the secure domain name service limitation. In both cases, the domain name is resolved to an IP address that is passed back to the client computer. See page 12, which discusses an "IP address provided by the application." This is corroborated by RFC 1035, the

standard for Internet domain name resolution, at least at page 4.



The final limitation of claim 1 requires, “sending an access request message to the secure computer network address using a virtual private network communication link.” Aventail discloses such a feature at page 8. A VPN according to Aventail is established so that the client computer can securely access resources using a public network. As introduced above, the subject matter recited in claim 1 of the ‘180 patent is fully disclosed in Aventail.

Claims 4, 10, and 12-15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the Aventail Administrator’s Guide, as shown in Appendix A. In brief illustration of select claims (Appendix A provides details for every claim):

For example, claim 4 recites that the response message contains provisioning information for the virtual private network. While the ‘180 patent does not expressly disclose “provisioning information,” Aventail , at least at pages 68, 69, and 77, discloses that Aventail Connect provides link, authentication, and access control information to allow secure access to a final destination across multiple firewalls of a network.

Claim 10 recites that the virtual private network includes the Internet, which Aventail discloses at pages 5, 8, and 79.

Claim 12 recites the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Aventail at least at pages 8 and 69.

Claim 14 recites that the method of claim 1 (see above) is performed by a software

module, and claim 15 recites that the method of claim 1 is performed by a client computer. Aventail is installed at the client computer and performs the method of claim 1. Aventail receives the secure domain name at the client computer, sends the name for resolution, receives the IP address, and issues the access request to the secure computer network address. See claim 1. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in Aventail.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix A, it is respectfully asserted that each of the limitations of claims 4, 10, and 12-15 is fully disclosed in Aventail, which therefore anticipates each of claims 4, 10, and 12-15.

Independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. In particular, claim 17 recites:

17. A computer-readable storage medium, comprising:
 - a storage area; and
 - computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.

As discussed above regarding claim 1, the Aventail Administrator's Guide discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Aventail discloses that the program code for Aventail is available by CD or can be delivered by network - i.e., computer readable instructions. See Aventail at page 14. Such computer code would be installed into a storage area at the client. Accordingly, Aventail fully anticipates the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include

further limitations that are disclosed in Aventail, as shown in Appendix A. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12-15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 1, 4, 10, and 12-15, and based on the citations presented in Appendix A, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed in Aventail, which therefore anticipates each of claims 20, 26, and 28 - 31.

Independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. In particular, claim 33 recites:

33. A data processing apparatus, comprising:
a processor, and
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:
receiving a secure domain name;
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
sending an access request message to the secure computer network address using a virtual private network communication link.

As discussed above regarding claim 1, Aventail discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Aventail discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Aventail at pages 7, 8, 13, and 72. Accordingly, Aventail fully anticipates the limitations of claim 33.

Claim 35 depends directly or ultimately from claim 33 and includes further limitations that are disclosed in Aventail, as shown in Appendix A. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based on the citations presented in Appendix A, it is respectfully asserted that each of the

limitations of claim 35 is fully disclosed in Aventail, which therefore anticipates claim 35.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Aventail Administrator's Guide prior art reference.

SNQ #2 Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 103(a) for being obvious over VPN Overview in view of RFC 1035

1. Substantial New Question of Patentability

VPN Overview/RFC 1035's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the VPN Overview and RFC 1035 teachings are "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, the VPN Overview/RFC 1035 combination discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

VPN Overview is another prior art reference that discusses the PPTP feature offered by Windows NT 4.0, prior to the filing date of the '180 patent. In addition to PPTP, VPN Overview further discloses the use of L2TP and IPsec for creating virtual private networks across the Internet. Connection requests for a secured domain name arrive at, for example, a VPN tunnel server, which resolves addresses against the Windows NT Domain Controller. (p. 27) Once resolved, the local resource's credentials are authenticated and a virtual private network is automatically created between the local resource and the remote resource. (p. 22).

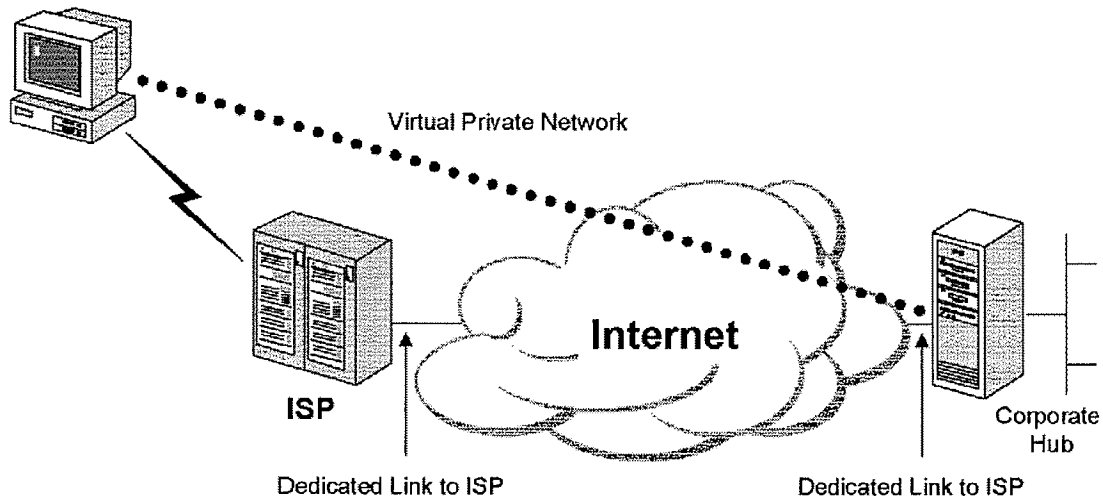
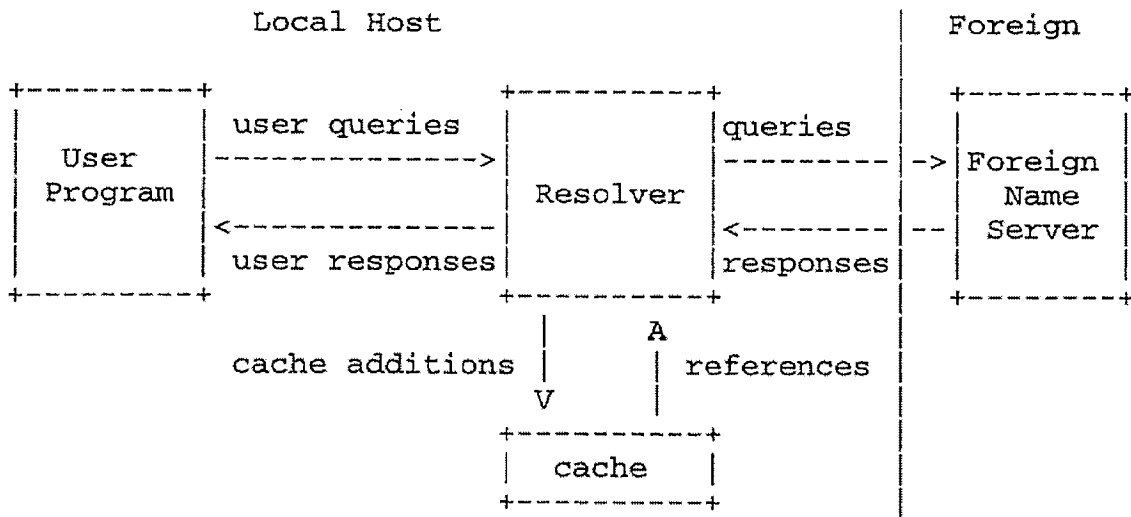


Figure 2: Using a VPN to connect a remote client to a private LAN

RFC 1035 specifies the standard for domain name resolution of Internet domain names. Upon receiving a domain name, the client computer passes the domain name to a resolver or name server to resolve the domain name to an IP address. Once resolved, the IP address is passed back to the requesting computer, which can then make a connection to the IP address. See RFC 1035 at page 4:



3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure

domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the VPN Overview reference or the RFC 1035 reference, which were respectively published in 1998 and 1987, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the VPN Overview reference, which was published in 1998; and the RFC 1035 reference, which was published in 1987, are both prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in the VPN Overview and the RFC 1035 references is attached hereto as Appendix B.

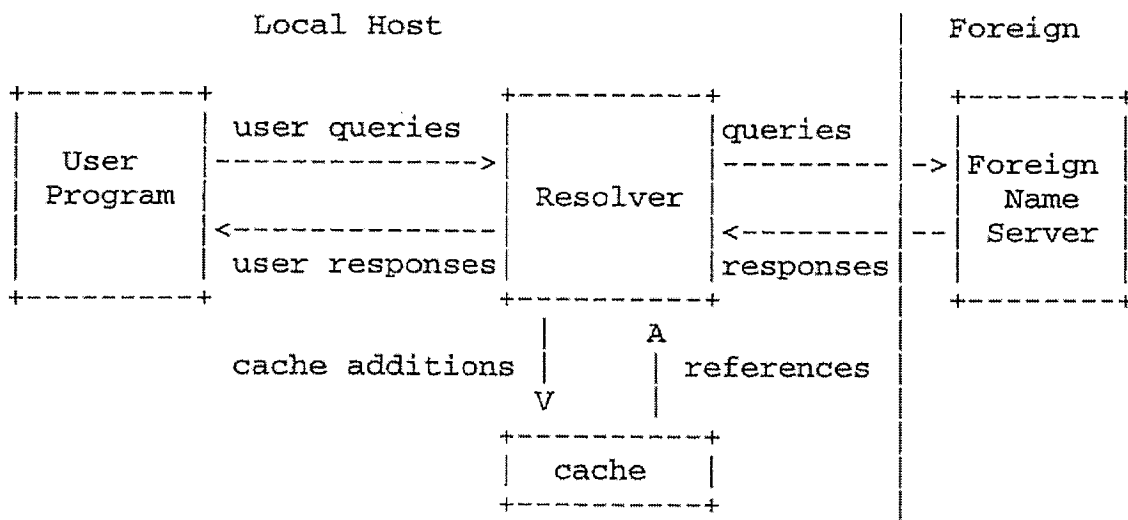
The preamble of claim 1 requires “a method for accessing a secure computer network address.” VPN Overview discloses such a feature at page 6. According to the Court in the Litigation, a “secure computer network address” means “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” Exhibit 13 at page 28. VPN Overview discloses at page 9 that authentication may be required before access is granted to resources at the remote service.

Claim 1 further requires, “receiving a secure domain name.” According to the Court in the Litigation, a “secure domain name” means “a domain name that corresponds to a secure computer network address.” Exhibit 13 at page 30. VPN tunnel servers can be identified using domain names. See page 26, which illustrates that a VPN tunnel server can be named “vpn.support.bigcompany.com.” This name corresponds to a secure network address – i.e., the address require authorization. The client computer receives this domain name from the user when the user identifies to where the VPN connection is to be made.

Claim 1 then requires “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” The Court in the Litigation construes “secure domain name service” broadly to include “a lookup service that returns a secure network

address for a requested secure domain name.” Exhibit 13 at page 32. Accordingly, a “secure domain name service” includes any lookup service that resolves a secure domain name.

As mentioned previously, VPN Overview discloses that VPN tunnel servers may be identified using domain names. There is further disclosure in VPN Overview at pages 6 and 7 discussing connections made over the Internet. RFC 1035 teaches that, in order to make a connection to an Internet domain name, the domain name is sent to a domain name service for resolution and then passed back the IP address. RFC 1035 at page 4:



Accordingly, RFC 1035 discloses the limitation.

The next limitation of claim 1 requires, “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.” RFC 1035 discloses at page 4 that the domain name is resolved and passed back as part of the user response.

The final limitation of claim 1 requires, “sending an access request message to the secure computer network address using a virtual private network communication link.” See VPN Overview at pages 6 - 10, 12, 14, 22, and 26 - 28. The purpose of the VPN is to access information at the VPN tunnel server using a VPN communication link. As introduced above, the subject matter recited in claim 1 of the ‘180 patent is fully disclosed in VPN Overview and RFC 1035.

Claims 4, 10, and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the VPN Overview or the RFC 1035 references, as shown in

Appendix B. In brief illustration of select claims (Appendix B provides details for every claim):

Claim 4 recites that the response message contains provisioning information for the virtual private network. VPN Overview, at least at pages 9, 26, and 27, discloses this feature. Information is exchanged between the computers to set up the VPN.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in the VPN Overview reference at least at page 6.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in VPN Overview at least at pages 6 and 7. For example, VPN Overview describes that one use of the VPN is to permit users to work remotely – i.e., use resources at the corporate site while at home or on the road.

Claim 14 recites that the method of claim 1 (see above) is performed by a software module, and claim 15 recites that the method of claim 1 is performed by a client computer. VPN Overview discloses a method for accessing a secure computer network address across a virtual private network. See VPN Overview at page 6 and as in Appendix B. VPN Overview also discloses receiving at a software module (i.e., Windows NT client) on a client computer a domain name for a secure remote computer and sending the domain name to a Domain Name System server for requesting a secure IP address corresponding to the domain name. See VPN Overview at pages 6, 7, and 26 - 27. VPN Overview discloses the use of DNS. As outlined in RFC 1035, DNS includes returning the IP address to the client computer. See RFC 1035 at least at pages 3, 4, and 20 - 21. Finally, a request is made from the software module at the client computer to connect to the specified remote computer via a secure virtual private network. See VPN Overview at pages 6 - 10, 12, 14, 22, and 26 - 28. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in the VPN Overview and RFC 1035 references.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix B, it is respectfully asserted that each of the limitations of claims 4, 10, and 12 - 15 is fully disclosed in the VPN Overview or RFC 1035 references.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-

readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the VPN Overview/RFC 1035 combination discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. VPN Overview, furthermore, discloses the well-known use of computer memory to store information, at least at pages 10 and 21. Computer-readable instructions are well-known parts of computer software application programs, which the systems described in VPN Overview are using. See VPN Overview at pages 10 and 21. Accordingly, the VPN Overview/RFC 1035 combination fully discloses the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in the VPN Overview and RFC 1035 references, as shown in Appendix B. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix B, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed in the VPN Overview and RFC 1035 references, which therefore render each of claims 20, 26, and 28 - 31 obvious.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the VPN Overview/RFC 1035 combination discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, VPN Overview discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See VPN Overview at pages 10 and 21. Accordingly, the VPN Overview/RFC 1035 combination renders claim 33 obvious.

Claim 35 depends directly from claim 33 and includes further limitations that are disclosed in the VPN Overview or RFC 1035 references, as shown in Appendix B. The limitations recited in claim 35 maps closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claims 4, and based upon the citations presented in Appendix B, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in the VPN

Overview and RFC 1035 references, which therefore render claim 35 obvious.

There are several reasons to combine the VPN Overview and RFC 1035 references in the manner discussed above to render claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 obvious. *KSR Int'l v. Teleflex, Inc.*, 127 S.Ct. 1727, 1733, 1743-44. A person of ordinary skill in the art of secure network communication, at the time the '180 patent was filed, and in possession of the VPN Overview reference would want to know the protocol and technique for obtaining the network address through the domain name service should a domain name be available. The RFC 1035 document, published more than ten years before both the publication of the VPN Overview reference and the filing of the '180 patent, would provide this sought-after information. It would only make sense for this skilled artisan to have drawn on the RFC 1035 protocols for obtaining the IP address of the domain name and returning it to the user in response to the query. By doing so, the artisan would be taking advantage of known methodologies for obtaining the network address to communicate with the requested domain.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore obvious under 35 U.S.C. § 103(a) by the VPN Overview and RFC 1035 references.

SNQ #3 Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 102(b) for being anticipated by Kosiur

1. Substantial New Question of Patentability

Kosiur's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Kosiur teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Kosiur discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Kosiur describes the building, operation, and management of virtual private networks over the Internet. Pages 37 and 40-42. Virtual private networks are created by establishing a “tunnel” through the Internet between two resources:

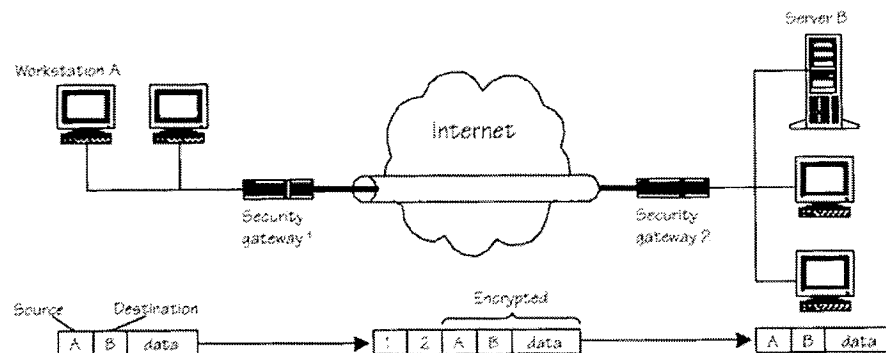


FIGURE 3.2 Schematic of a tunnel.

Tunnels can be established in several different ways. In relevant part to the ‘180 patent, Kosiur acknowledges that VPNs often use DNS servers to resolve connection requests. Page 36.

For example, a corporation may keep an internal DNS server for resolving VPN requests behind a firewall and a second VPN DNS server outside the firewall. (p. 296). When a connection request for a secured resource outside the firewall is made, the internal VPN DNS server forwards the connection request to the external DNS server. (p. 296). The domain name is resolved and the external DNS server negotiates the connection request and establishes a VPN between the local and remote sources. (p. 47, 297).

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in Kosiur, which was published in 1998, before the April 26, 2000 filing of the ‘209 CIP patent application. As discussed above, the disclosure

of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the 1998 Kosiur is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in the Kosiur is attached hereto as Appendix C.

The preamble of claim 1 requires “a method for accessing a secure computer network address.” Kosiur discloses such a feature at pages 37 and 41-42, which discuss the use of a VPN to secure communications across a network such as the Internet. According to the Court in the Litigation, a “secure computer network address” means “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” Exhibit 13 at page 28. Kosiur disclose at pages 47 and 132 that authentication may be required before access is granted to resources at the remote service.

Claim 1 further requires, “receiving a secure domain name.” According to the Court in the Litigation, a “secure domain name” means “a domain name that corresponds to a secure computer network address.” Exhibit 13 at page 30. Kosiur is replete with references to domain name usage with VPN enabled servers and computers. See, for example, pages 293-296. These domain names are “secure” according to the Court’s construction because the domain names correspond to network addresses that require authentication. These names are received at the client computer from a user attempting to reach the named site.

Claim 1 then requires “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” The Court in the Litigation construes “secure domain name service” broadly to include “a lookup service that returns a secure network address for a requested secure domain name.” Exhibit 13 at page 32. Accordingly, a “secure domain name service” includes any lookup service that resolves a secure domain name.

As mentioned in a previous paragraph, Kosiur discloses Internet domain names for identifying VPN resources. When a user enters a domain name at the client computer, the client computer issues a lookup request to a domain name service server. See pages 293-296.

The next limitation of claim 1 requires, “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure

domain name.” Kosiur discloses at pages 293-296 that domain name resolution occurs at DNS servers. The DNS servers pass back the corresponding network address.

The final limitation of claim 1 requires, “sending an access request message to the secure computer network address using a virtual private network communication link.” See Kosiur at pages 40-42. The purpose of the VPN is to access information across a network connection, which requires sending an access request message over the established VPN link to the IP address at the far end. As introduced above, the subject matter recited in claim 1 of the ‘180 patent is fully disclosed in Kosiur.

Claims 4, 10, and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in Kosiur, as shown in Appendix C. In brief illustration of select claims (Appendix C provides details for every claim):

Claim 4 recites that the response message contains provisioning information for the virtual private network. Kosiur, at least at pages 40 - 42, 132, 296, 308 - 309, and 311, discloses the RSVP feature for providing information for allocating and reserving network resources and paths for the network.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in Kosiur at least at page 379.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. Kosiur discloses at least at pages 40 – 42, 133, and 276 - 277 the feature of requesting data or requesting authentication information to establish a secure link.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. Kosiur discloses a method for accessing a secure computer network address across a virtual private network. See Kosiur at pages 37, 40 - 42, and 379 and as in Appendix C. Kosiur discloses receiving at a software module (i.e., Windows NT client or server – depending on which computer is acting as the “client”) on a client computer a domain name for a secure destination computer and sending the domain name to a Domain Name Service server for converting the domain name into a secure IP address. See Kosiur at pages 216, and 293 - 294. The IP address is returned to the software module at the client computer, and a request is made from the software module to create the secure connection to the specified destination computer. See Kosiur at pages 40 - 42, 47, and 296. As introduced

above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in the Kosiur reference.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix C, it is respectfully asserted that each of the limitations of claims 4, 10, and 12 - 15 is fully disclosed in Kosiur, which therefore anticipates each of claims 4, 10, and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Kosiur discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Kosiur discloses the well-known use of computer memory to store information at least at pages 111 and 162. Computer-readable instructions correspond to the software performing the functions disclosed in the reference. See Kosiur at page 111. Accordingly, Kosiur fully anticipates the limitations of claim 17.

Claims 20, 26 and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in Kosiur, as shown in Appendix C. The limitations recited in claims 20, 26 and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix C, it is respectfully asserted that each of the limitations of claims 20, 26 and 28 - 31 is fully disclosed in Kosiur, which therefore anticipates each of claims 20, 26 and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Kosiur discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Kosiur discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Kosiur at pages 34, 37, and 40 - 42. Accordingly, Kosiur fully anticipates the limitations of claim 33.

Claim 35 depends directly or ultimately from claim 33 and includes further limitations that are disclosed in Kosiur, as shown in Appendix C. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix C, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in Kosiur, which therefore anticipates claims 35. For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(b), by the Kosiur prior art reference.

SNQ #4 Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Kaufman

1. Substantial New Question of Patentability

Kaufman's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Kaufman teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Kaufman discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Kaufman is a reference disclosing the use of IPsec to secure communications through the Internet using authentication and encryption. IPsec is a framework of standards for helping to ensure private, secure communications by supporting network-level data integrity, data confidentiality, data origination authentication, and replay protection. In relevant part to the '180 patent, Kaufman discloses methods for tunneling through the Internet to create a virtual private

network between two resources. Pages 141-142. These resources can be on the Internet, an intranet, an extranet, or mobile network.

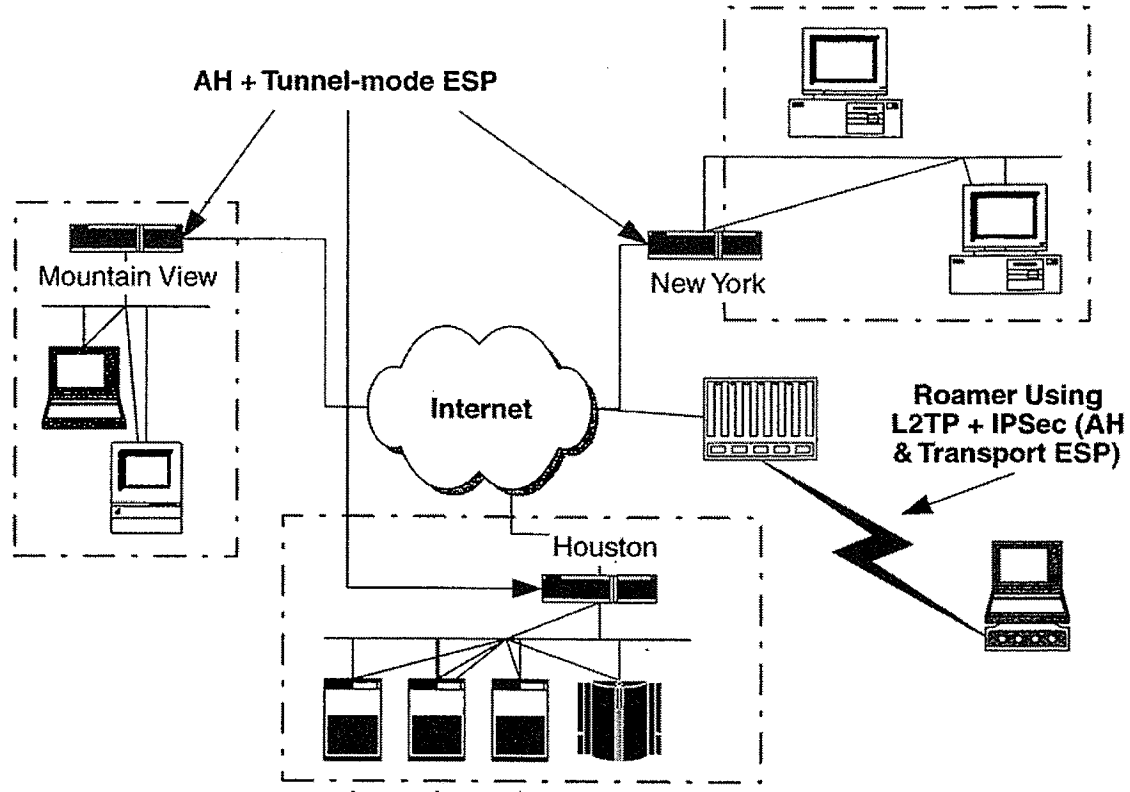


Figure 9.1 IPsec VPN.

In practice, an IPsec connection request over the Internet for a secured resource can use, for example, a DNS server to resolve the request. (p. 127). Once the secured domain name is resolved, a connection can be established between the secured resource and the computer requesting the connection. IPsec includes two basic security protocols: an authentication header and an encapsulating security payload. (p. 78). The secured resource verifies the authenticity of the sender, and a connection is established. (p. 78).

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing

the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Kaufman reference, which was published in 1999, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the 1999 Kaufman reference is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Kaufman is attached hereto as Appendix D.

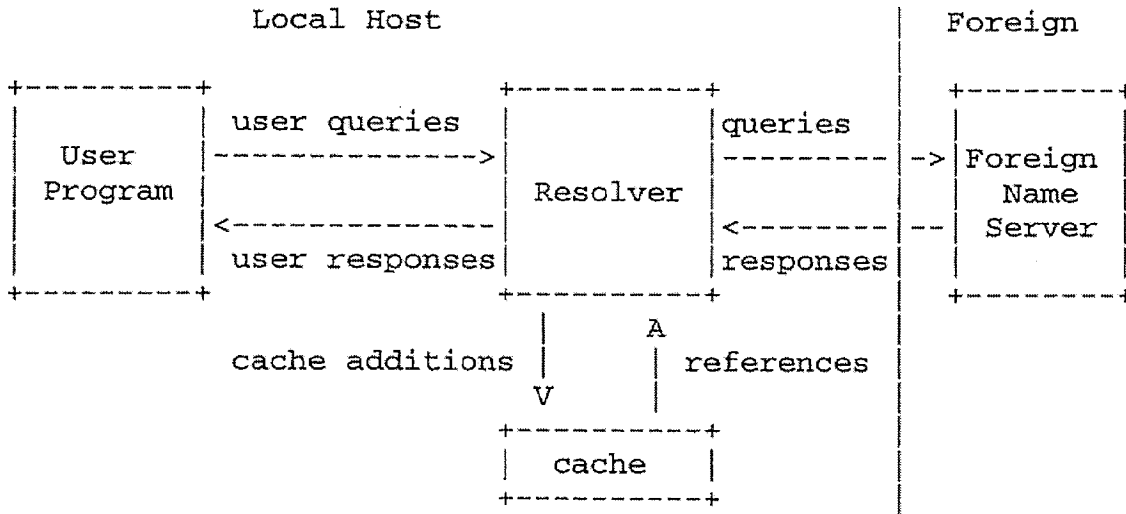
The preamble of claim 1 requires “a method for accessing a secure computer network address.” Kaufman discloses the use of IPsec to create a VPN extranet over the Internet at pages 140-142. According to the Court in the Litigation, a “secure computer network address” means “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” Exhibit 13 at page 28. Kaufman discloses that IPsec includes several different mechanisms for authenticating users before access is granted to resources at the remote service. See at least pages 2 and 9.

Claim 1 further requires, “receiving a secure domain name.” According to the Court in the Litigation, a “secure domain name” means “a domain name that corresponds to a secure computer network address.” Exhibit 13 at page 30. As discussed concerning the preamble, Kaufman discloses that IPsec includes secure computer network addresses. Kaufman further discloses that the secure computer network addresses can be referenced using domain names. See page 127. Accordingly such domain names are “secure” domain names under the Court’s construction because the domain names correspond to secure computer network addresses. These names are received at the client computer from a user attempting to reach the name.

Claim 1 then requires “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” The Court in the Litigation construes “secure domain name service” broadly to include “a lookup service that returns a secure network address for a requested secure domain name.” Exhibit 13 at page 32. Accordingly, a “secure domain name service” includes any lookup service that resolves a secure domain name.

As mentioned in a previous paragraph, Kaufman discloses Internet domain names for identifying IPsec resources. When a user enters a domain name at the client computer, the client computer issues a lookup request to a domain name service server to resolve an IP address from a domain name and to enable secure communication over the network. See pages 125, 127, 128, 143 - 144, 191, and 243. Kaufman also discloses the use of DNSSEC as the standards and security mechanisms specific to domain name services. See page 128.

The next limitation of claim 1 requires, “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.” Kaufman at pages 125, 127, 128, and 191 discuss the use of DNS. In DNS, the resolution server passes back the corresponding network address. RFC 1035 provides corroboration at page 4:



The final limitation of claim 1 requires, “sending an access request message to the secure computer network address using a virtual private network communication link.” See Kaufman at pages 140-142. The purpose of the IPsec is to permit the secure access information across a public network connection using a virtual private network. As introduced above, the subject matter recited in claim 1 of the ‘180 patent is fully disclosed in Kaufman.

Claims 4, 10 and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in Kaufman, as shown in Appendix D. In brief illustration of select claims (Appendix D provides details for every claim):

For example, claim 4 recites that the response message contains provisioning information

for the virtual private network. Kaufman, at least at page 121, discloses this feature.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in Kaufman at least at page 126.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Kaufman at least at pages 141 - 142.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. Kaufman discloses a method for accessing a secure computer network address across a virtual private network. See Kaufman at pages 140 - 144 and as in Appendix D. Kaufman also discloses receiving a domain name at a software module on a client computer (i.e., IPsec host computer) for a secure destination computer and sending the domain name to a Domain Name System server for resolving the domain name to a secure IP address. See Kaufman at pages 125, 127, 128, 191, and 243. The IP address is returned to the software module at the client computer, and a request is made to begin the secure connection to the specified destination computer. See Kaufman at pages 125, 127, 128, 191, and 243. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in Kaufman.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix D, it is respectfully asserted that each of the limitations of claims 4, 10 and 12 - 15 is fully disclosed in Kaufman, which therefore anticipates each of claims 4, 10 and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Kaufman discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Kaufman discloses the well-known use of computer memory to store information at least at page 215. Computer-readable instructions correspond to the software performing the functions disclosed in the reference. See Kaufman at pages 103, 104, 143, and 144. Accordingly, Kaufman fully anticipates the limitations of claim 17.

Claims 20, 26 and 28 - 31 depend directly or ultimately from claim 17 and include further

limitations that are disclosed in Kaufman, as shown in Appendix D. The limitations recited in claims 20, 26 and 28 - 31 map closely to the limitations recited in claims 4, 10 and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10 and 12 - 15, and based upon the citations presented in Appendix D, it is respectfully asserted that each of the limitations of claims 20, 26 and 28 - 31 is fully disclosed in Kaufman, which therefore anticipates each of claims 20, 26 and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Kaufman discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Kaufman discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Kaufman at pages 103, 104, 141, and 142. Accordingly, Kaufman fully anticipates the limitations of claim 33.

Claim 35 depends directly or ultimately from claim 33 and includes further limitations that are disclosed in the Kaufman, as shown in Appendix D. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix D, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in Kaufman, which therefore anticipates claim 35.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Kaufman prior art reference.

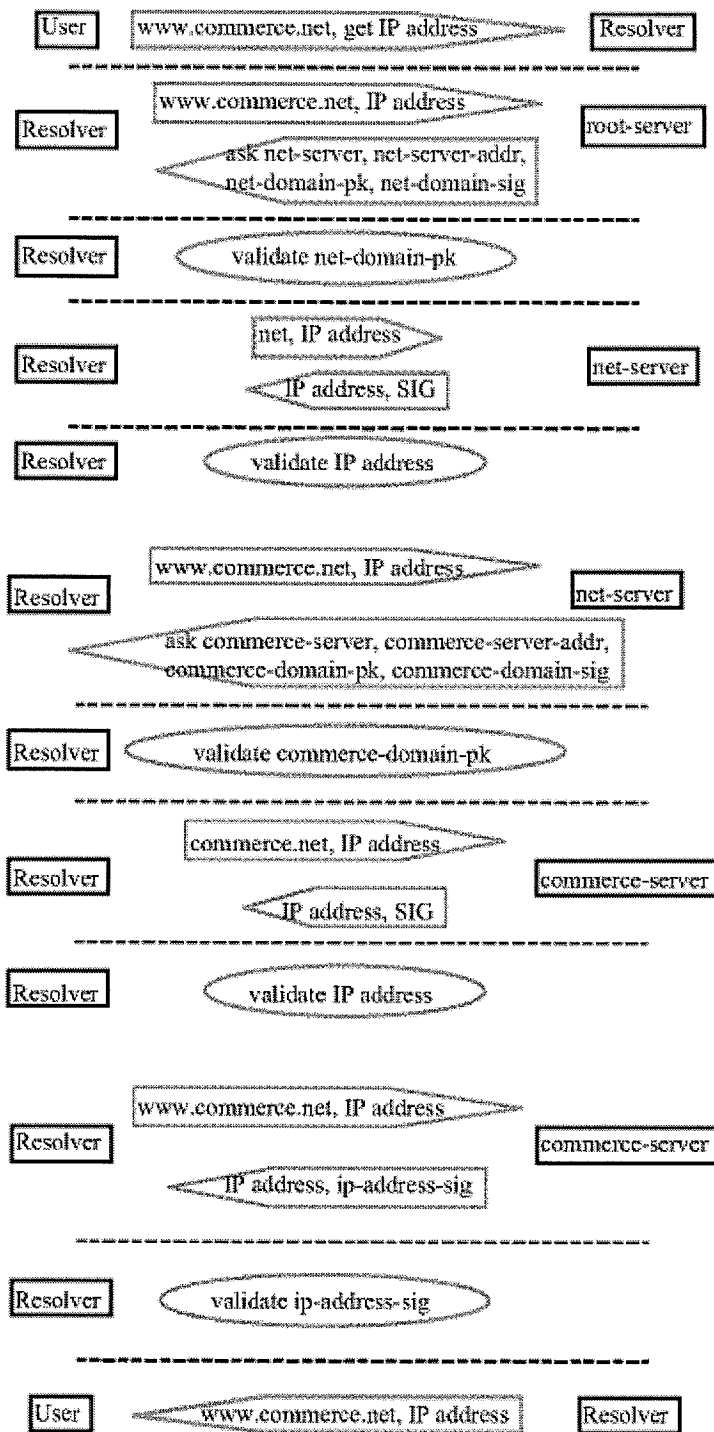
SNQ #5 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103 for being obvious over Kaufman in view of Galvin**

1. Substantial New Question of Patentability

Kaufman/Galvin’s disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the ‘180 patent application (*i.e.*, the Kaufman and Galvin teachings are “new”). In particular, it is submitted that, based on the Examiner’s statement of reasons for allowance, the claims of the ‘180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, the Kaufman/Galvin combination discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Kaufman is described above in Section V(SNQ #4). Galvin discusses a second type of secure domain name service that enhances the security of the Domain Name System by cryptographically binding domain names to their resources. Page 5. Specifically, Galvin discloses that the resource records managed by the DNS are digitally signed. Section 3.2 of Galvin provides an example of a DNS lookup where the DNS is secured with digitally signed records. A user issues a DNS lookup request to the local resolver, which sends the request along with a public key to the root server. The root server, in this case, does not have the necessary information for the DNS lookup; so it directs the local resolver to look to the net-domain for the lookup information. The local resolver can trust the response from the root server (*i.e.*, the root server is secure) because the resolver and the root server share the appropriate public and private keys to the signed records. Eventually the resolver is directed to a DNS server that can answer the DNS lookup request. As before, the local resolver can trust that the DNS server is secure based on the successful validation of the public key.



3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Kaufman reference as described above in Section V(SNQ #4). Each of the steps of claim 1 are also disclosed between the Kaufman and Galvin references, which are the subject of this SNQ. The Kaufman and Galvin references were published in 1999 and 1996, respectively, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the Kaufman and Galvin references are prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Kaufman and Galvin is attached hereto as Appendix E.

Kaufman's applicability to the claims is discussed in SNQ #4 and will not be repeated here. Galvin provides a second type of "secure domain name service" that includes digitally signed resource records. Secure domain name service is relevant for the following limitations in claim 1 (and the respective counterparts in claims 17 and 33):

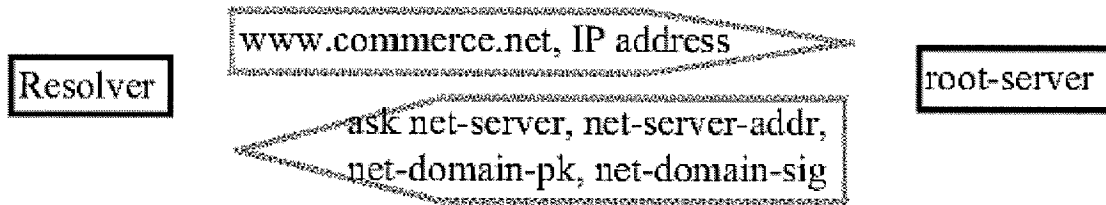
send a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name,

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name

Galvin discloses these limitations at, for example, section 3.2, which discusses an example where a user issues a DNS lookup request for www.commerce.net. According to the example, the user issues a query message to the local resolver requesting the IP address corresponding to www.commerce.net.



The local resolver is forwarded to several different DNS servers until a DNS server is reached that contains the corresponding IP address.



At each step, the local server validates the DNS server using the public key.



The appropriate DNS server returns the IP address corresponding to the domain name in the DNS lookup request.



Accordingly, when the type of secure DNS server disclosed in Galvin receives the DNS lookup request described in Kaufman, the secure DNS service will return the secure IP address corresponding to the request. This combination, therefore, meets the Court’s construction in the Litigation that a “secure domain name service” means “a lookup service that returns a secure network address for a requested secure domain name.” Exhibit 13 at page 32.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the ‘180 patent is fully disclosed, and therefore rendered obvious under 35 U.S.C. § 103, by the Kaufman reference in view of the Galvin reference.

It would have been obvious to one of ordinary skill in the art to combine the Kaufman and Galvin references because one of ordinary skill in the art would have recognized that such a combination would have provided the predictable result of improving Kaufman. More particularly, Galvin discloses that its DNS “enhances or adds to the existing DNS, as opposed to

changing or removing from the existing DNS.” Galvin at page 8.

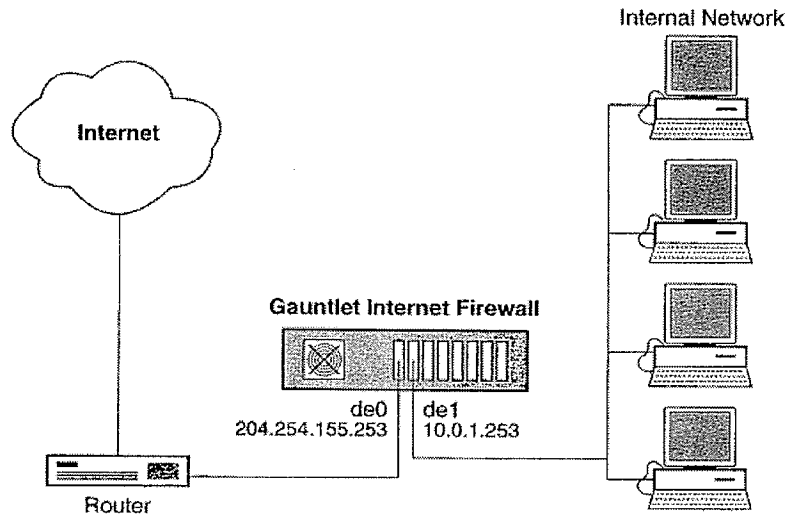
SNQ #6 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Gauntlet**

1. Substantial New Question of Patentability

Gauntlet’s disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the ‘180 patent application (*i.e.*, the Gauntlet teaching is “new”). In particular, it is submitted that, based on the Examiner’s statement of reasons for allowance, the claims of the ‘180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Gauntlet discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Gauntlet is the administrator guide for the Gauntlet Firewall for Windows NT product and is another prior art reference discussing PPTP. In particular, Gauntlet discusses PPTP in the context of firewalls and security services. Gauntlet Firewall includes several security services for a number of popular applications - e.g. HTTP, PPTP, LDAP, FTP, and POP3. Each application generally talks through a different proxy service at the firewall. When traffic arrives at the firewall, the firewall evaluates whether the traffic is permitted. If it is, the traffic is passed to the appropriate proxy. PPTP, as previously mentioned, is one such proxy service offered by the Gauntlet Firewall and is described in detail beginning at page 18-1.



3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Gauntlet reference, which was published no later than 1999, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the 1999 Gauntlet is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in the Gauntlet reference is attached hereto as Appendix F.

The preamble of claim 1 requires “a method for accessing a secure computer network address.” Gauntlet at page 18-1 discloses that PPTP connections can be established using the firewall . According to the Court in the Litigation, a “secure computer network address” means “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” Exhibit 13 at page 28. Gauntlet at pages 1-

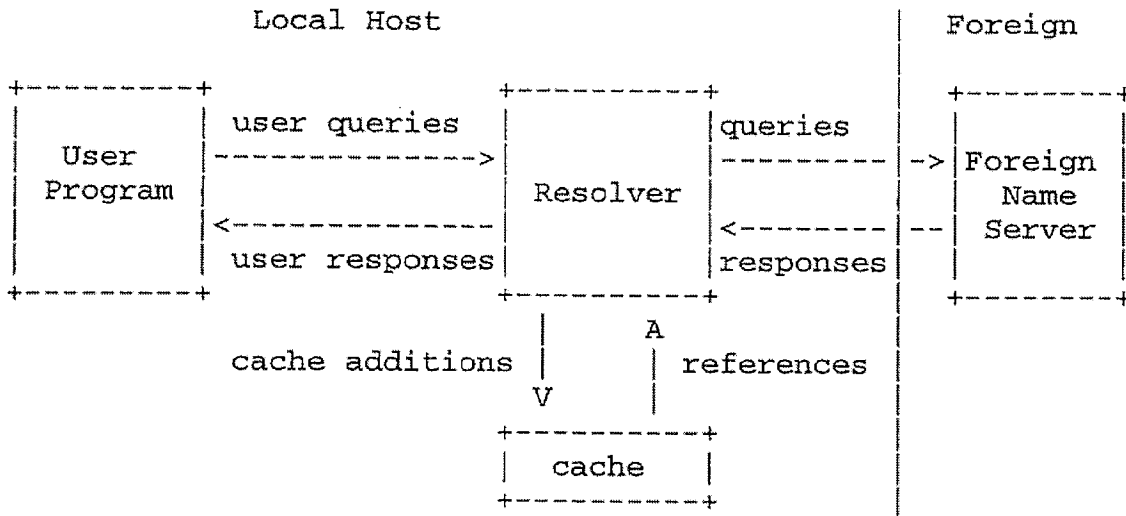
9 and 28-2 discloses that authentication may be required before access is granted to resources at the remote service.

Claim 1 further requires, “receiving a secure domain name.” According to the Court in the Litigation, a “secure domain name” means “a domain name that corresponds to a secure computer network address.” Exhibit 13 at page 30. PPTP connections can be identified using domain names. See Gauntlet at pages 5-1, 5-2, 5-4, 20-1, and G-1, which illustrate that remote resources can be located using the domain name service. In the case where the domain name corresponds to a PPTP enabled server, the domain name is a secure domain name according to the Court’s construction because the domain name corresponds to a secure network address (i.e., an address requiring authentication).

Claim 1 then requires “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” The Court in the Litigation construes “secure domain name service” broadly to include “a lookup service that returns a secure network address for a requested secure domain name.” Exhibit 13 at page 32. Accordingly, a “secure domain name service” includes any lookup service that resolves a secure domain name.

Gauntlet discloses at pages 5-1, 5-2, 5-4, 20-1, and G-1 that the firewall includes a domain name services server to resolve domain names to corresponding network addresses. This DNS is a “secure” DNS according to the Court’s construction because the DNS resolves a domain name for a PPTP enabled server.

The next limitation of claim 1 requires, “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.” Gauntlet discloses such a feature at pages 5-1, 5-2, 5-4, 20-1, and G-1. As discussed in the previous paragraph, the firewall includes a DNS server to handle domain name resolution. DNS servers return the IP address corresponding to the received domain name. This is corroborated by RFC 1035 at page 4:



The final limitation of claim 1 requires, “sending an access request message to the secure computer network address using a virtual private network communication link.”

Gauntlet discloses such a feature at page 18-1. The purpose of PPTP is to establish a VPN communication link so that the client computer can securely access resources using a public network. As introduced above, the subject matter recited in claim 1 of the ‘180 patent is fully disclosed in Gauntlet.

Claims 4, 10, and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in Gauntlet, as shown in Appendix F. In brief illustration of select claims (Appendix F provides details for every claim):

For example, claim 4 recites that the response message contains provisioning information for the virtual private network. The Gauntlet reference, at least at pages 1-8 and 18-1 - 18-4, discloses the feature of providing resource information for allocating network resources, including hosts and ports.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in the Gauntlet reference at least at pages 1-7 and 30-5.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Gauntlet at least at page 18-1.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. The Gauntlet reference discloses a method for accessing a secure computer network address across a virtual private network. See

Gauntlet at pages 1-4, 1-9, 18-1, and 30-5 and as in Appendix F. The Gauntlet reference discloses receiving a domain name at a software module (e.g., Internet browser, Windows NT, or other software that a user may use) on a client computer for a secure destination computer and sending the domain name to a Domain Name System server for mapping the domain name into a secure IP address. See Gauntlet at pages 1-8, 5-2, 18-1, and 30-5. The IP address is returned to the client computer, and a request is made to begin the secure connection to the specified destination computer. See Gauntlet at pages 1-7, 1-9, 5-1, 5-2, 5-4, 18-1, 20-1, and G-1.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix F, it is respectfully asserted that each of the limitations of claims 4, 10, and 12 - 15 is fully disclosed in the Gauntlet reference, which therefore anticipates each of claims 4, 10, and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Gauntlet reference discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, the Gauntlet discloses the well-known use of computer memory to store information at least at pages 1-7, 10-1, and 18-1. While the Gauntlet reference does not expressly disclose computer-readable instructions, neither does the '180 patent; and such instructions are well-known parts of computer software application programs. See Gauntlet at pages 1-1 and 1-4. Accordingly, the Gauntlet reference fully anticipates the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in the Gauntlet, as shown in Appendix F. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix F, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed in the Gauntlet reference, which therefore anticipates each of claims 20, 26, and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to

subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Gauntlet discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, the Gauntlet reference discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Gauntlet at pages 1-1, 1-7, and 18-1. Accordingly, the Gauntlet reference fully anticipates the limitations of claim 33.

Claim 35 depends from claim 33 and include further limitations that are disclosed in the Gauntlet reference, as shown in Appendix F. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix F, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in the Gauntlet reference, which therefore anticipates claim 35.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Gauntlet prior art reference.

SNQ #7 Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 103(a) for being obvious over Hands On in view of Installing NT

1. Substantial New Question of Patentability

Hands On/Installing NT's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Hands On and Installing NT teachings are "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which

is an element recited in independent claims 1, 17, and 33. As discussed below, the Hands On/Installing NT combination discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Long before the applicant filed the application that became '180 patent, the Windows NT 4.0 software system included a virtual private networking protocol called PPTP. PPTP, as described in Hands On and Installing NT, is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server, thus creating a virtual private network (VPN) over TCP/IP-based data networks, including local area networks (LANs), wide area networks (WANs), and the Internet and other public, TCP/IP-based networks.

PPTP requires the installation and configuration of the PPTP software at both the client computer and the PPTP server. Once configured, the user at the client computer creates a "phonebook" entry that contains the necessary details for the client computer to establish a PPTP connection with the PPTP server. The entry includes the PPTP server domain name, IP address, and other information.

In addition to the PPTP network protocol, the Windows NT 4.0 software system included an automatic dialing feature called AutoDial. AutoDial, as described in Hands On, is a feature that remembers the network connections made by users at the client computer and automatically configures these connections the next time the client computer makes the same connection request. AutoDial remembers these connections by mapping connection requests to their respective phonebook entries. In practice, a user requests a particular destination using the command line or alternatively, using an icon. See Hands On at page 462. AutoDial takes this input, recognizes the destination, and launches the appropriate phonebook entry.

Between these two features, Windows NT 4.0, as described by Hands On and Installing NT discloses a method for access a secure computer network according to the '180 patent.

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing

the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Hands On or Installing NT references, which were published in 1998 and 1997, respectively, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, Hands On and Installing NT are prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Hands On and Installing NT is attached hereto as Appendix G.

The preamble of claim 1 requires “a method for accessing a secure computer network address.” Hands On discloses such a feature at page 432. PPTP is a network protocol for accessing PPTP enabled network addresses. According to the Court in the Litigation, a “secure computer network address” means “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” Exhibit 13 at page 28. Hands On discloses at pages 435, 438, and 447 that Windows NT clients and servers may require authentication before access is granted to resources at the remote service.

Claim 1 further requires, “receiving a secure domain name.” According to the Court in the Litigation, a “secure domain name” means “a domain name that corresponds to a secure computer network address.” Exhibit 13 at page 30. PPTP connections can be identified using domain names. See figure below from page 21 of Installing NT, which illustrates that a PPTP server can be named “pptpserver.mycompany.com.” This name corresponds to a secure network address – i.e., the address of the PPTP server. The client computer receives the domain name from the user in the form of a command line or icon.

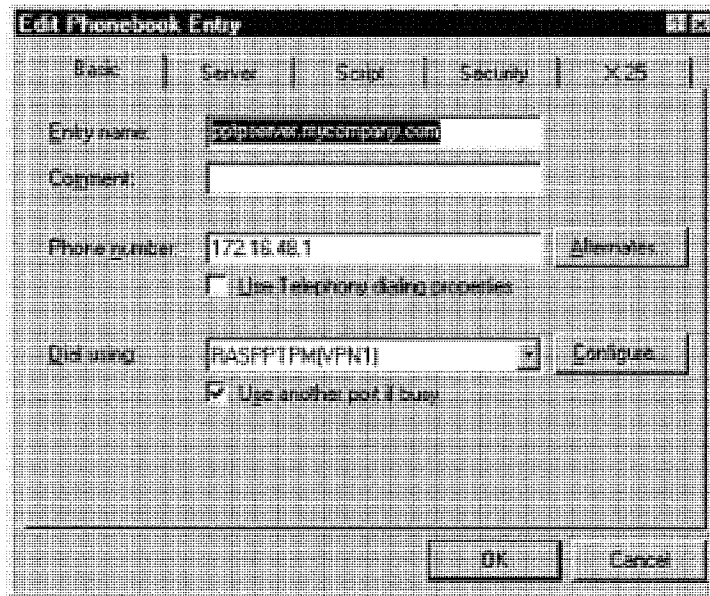


Figure 12 - Example Phonebook entry for PPTP server and a VPN device

Claim 1 then requires “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” The Court in the Litigation construes “secure domain name service” broadly to include “a lookup service that returns a secure network address for a requested secure domain name.” Exhibit 13 at page 32. Accordingly, a “secure domain name service” includes any lookup service that resolves a secure domain name.

There are two “lookup services” described in Hands On that independently satisfy this limitation. The first “lookup service” is the traditional DNS server as defined by the Internet Engineering Task Force (IETF). Hands On discloses this feature at page 401 in an aptly named section called “How DNS Works.” The first step is sending a query message to the DNS server requesting the corresponding IP address. Using the example in the figure above, when a user at the client computer tries to connect to “pptpserver.mycompany.com,” the client computer sends a request to the secure DNS server (i.e., one capable of resolving the domain name) to resolve the secure domain name to the IP address.

The alternative “lookup service” disclosed in Hands On is AutoDial. If AutoDial is configured properly, it will return the phonebook entry corresponding to the domain name. Put another way, the client computer can request from AutoDial the IP address, which is part of the phonebook entry. See Hands On at page 462, describing how AutoDial maps domain names to

corresponding IP addresses.

The next limitation of claim 1 requires, “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.” As discussed above, there are two “lookup services” disclosed in Hands On that independently satisfy the secure domain name service limitation. In both cases, the domain name is resolved to an IP address that is passed back to the client computer. With respect to the traditional DNS server, this is disclosed in Hands On at page 401. With respect to AutoDial, this is disclosed in Hands On at page 462, which describes how AutoDial maps domain names to their respective IP addresses. When AutoDial receives the domain name, it returns the appropriate phonebook entry with the IP address.

The final limitation of claim 1 requires, “sending an access request message to the secure computer network address using a virtual private network communication link.” Hands On discloses such a feature at page 431. The purpose of PPTP is to establish a VPN communications link so that the client computer can securely access resources using a public network. As introduced above, the subject matter recited in claim 1 of the ‘180 patent is fully disclosed in Hands On and Installing NT.

Claims 4, 10, and 12-15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the Hands On or Installing NT, as shown in Appendix G. In brief illustration of select claims (Appendix G provides details for every claim):

Claim 4 recites that the response message contains provisioning information for the virtual private network. Installing NT discloses in its abstract that PPTP can be used to establish secure virtual networks using dial-up lines, local area networks, wide area networks, or the Internet. A PPTP-enabled client computer must have at least two phonebook entries describing its access server ports, i.e., resources, to the VPN. Pages 20 - 23. The address of the servers can be specified by their IP address or through a domain name service. Page 21. Once the initial network access is made, the network responds with network resource information from a phonebook entry, including network protocols and particular network adapters. Pages 20 - 23. In the figure on page 21, the network adapter is identified as RASPPTPM(VPN1). Further on at page 20, there is additional provisioning information including the connection protocol (TCP/IP) and whether compression is enabled.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in

Hands On at least at page 431.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Hands On at least at page 431.

Claims 14 and 15 recite that the method is performed by a software module and that the method is performed by a client computer. More particularly, Windows NT 4.0, a software module, is installed at the client computer and configured for PPTP. Windows NT 4.0 receives a secure domain name from a user, sends the secure domain name for resolution, receives the corresponding secure network address, and subsequently sends an access request to the secure network address. See the discussion above regarding claim 1.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix G, it is respectfully asserted that each of the limitations of claims 1, 4, 10, and 12-15 is fully disclosed in the Hands On or Installing NT references, which therefore renders obvious each of claims 1, 4, 10, and 12-15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Hands On reference in view of Installing NT disclose each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Hands On discloses the well-known use of computer memory to store information at least at page 428. While Hands On does not expressly disclose computer-readable instructions, neither does the '180 patent; and such instructions are well-known parts of computer software application programs. See Hands On at page 428.

Accordingly, Hands On in view of Installing NT fully discloses the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in Hands On, as shown in Appendix G. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix G, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed by Hands On in view of Installing NT, which therefore

render obvious each of claims 20, 26, and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Hands On in view of Installing NT discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Hands On discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Hands On at page 428. Accordingly, Hands On in view of Installing NT fully anticipates the limitations of claim 33.

Claim 35 depends directly from claim 33 and includes a further limitation that is disclosed in Hands On, as shown in Appendix G. The limitation recited in claim 33 maps closely to the limitation recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix G, it is respectfully asserted that each of the limitations of claims 35 is fully disclosed in Hands On in view of Installing NT, which therefore renders claim 35 obvious.

There are several reasons to combine the Hands On and Installing NT references in the manner discussed above to render claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 obvious. See *KSR Int'l v. Teleflex, Inc.*, 127 S.Ct. 1727, 1733, 1743-44. First and foremost, both references concern the use of PPTP and Windows NT 4.0 for establishing VPNs. See Hands On at page 431 and Installing NT at abstract. One of ordinary skill in the art would have recognized that it would have been common sense to combine the references because they discuss the same product. Similarly, one of ordinary skill in the art would have recognized that the combination of the two references would have led to predictable results – again, because the references discuss the same product.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore rendered obvious under 35 U.S.C. § 103(a), by Hands On in view of Installing NT.

SNQ #8 Claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Microsoft VPN

1. Substantial New Question of Patentability

Microsoft VPN's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Microsoft VPN teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Microsoft VPN discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

The Microsoft VPN reference is another prior art reference regarding PPTP and discusses Virtual Private Networking technology in the context of Windows NT 4.0. In particular, Microsoft VPN discusses the use of VPNs for corporate users that are working remotely. The reference provides significant detail concerning the PPTP data packets, network routing concerns, and security. Figure 1 illustrates the logical concept of a VPN.

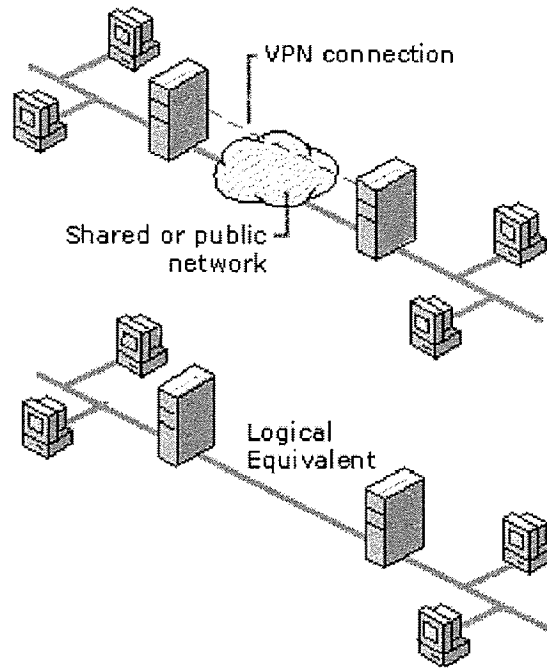


Figure 1 Virtual Private Network (VPN)

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Microsoft VPN reference, which was published January 1, 2000, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the Microsoft VPN is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 of the '180 patent as found in the Microsoft VPN reference is attached hereto as Appendix H.

The preamble of claim 1 requires "a method for accessing a secure computer network

address.” Microsoft VPN at page 11 discloses that PPTP connections can be established to secure communication paths across a public network. According to the Court in the Litigation, a “secure computer network address” means “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” Exhibit 13 at page 28. Microsoft VPN discloses that authentication may be required before access is granted to resources at the remote service. See page 13.

Claim 1 further requires, “receiving a secure domain name.” According to the Court in the Litigation, a “secure domain name” means “a domain name that corresponds to a secure computer network address.” Exhibit 13 at page 30. PPTP connections can be identified using domain names. See Microsoft VPN at page 32, which discloses that the VPN server can be addresses using either the host name or the IP address. In the case where the domain name corresponds to a PPTP enabled server, the domain names is a secure domain name according to the Court’s construction because the domain name corresponds to a secure network address (i.e., an address requiring authentication).

Claim 1 then requires “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” The Court in the Litigation construes “secure domain name service” broadly to include “a lookup service that returns a secure network address for a requested secure domain name.” Exhibit 13 at page 32. Accordingly, a “secure domain name service” includes any lookup service that resolves a secure domain name.

Microsoft VPN discloses that domain names are sent to a domain name services server for resolution. In other words, a query message is sent to the domain name services server for the IP address corresponding to the domain name. See pages 63 - 66. This DNS is a “secure” DNS according to the Court’s construction because the DNS resolves a domain name for a PPTP enabled server.

The next limitation of claim 1 requires, “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.” Microsoft VPN discloses such a feature at pages 63 - 66. DNS servers return the IP address corresponding to the received domain name.

The final limitation of claim 1 requires, “sending an access request message to the secure computer network address using a virtual private network communication link.” MS VPN

discloses such a feature at pages 11 - 12. The purpose of PPTP is to establish a VPN communication link so that the client computer can securely access resources using a public network. See Microsoft VPN at page 11. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in Microsoft VPN.

Claims 10 and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the Microsoft VPN, as shown in Appendix H. In brief illustration of select claims (Appendix H provides details for every claim):

Claim 10 recites the virtual private network includes the Internet, which is disclosed in the Microsoft VPN reference at least at page 34.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Microsoft VPN at least at page 11.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. The Microsoft VPN reference discloses a method for accessing a secure computer network address across a virtual private network. See Microsoft VPN at pages 11, 13, and 34 and as in Appendix H. The Microsoft VPN reference discloses receiving a domain name at a software module (i.e., Windows NT 4.0) on a client computer for a secure destination computer and sending the domain name to a Domain Name System server for mapping the domain name into a secure IP address. See Microsoft VPN at pages 11, 13, 32, and 35. The IP address is returned to the software module on the client computer, and a request is made to begin the secure connection to the specified destination computer. See Microsoft VPN at pages 11, 13, and 16. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in the Microsoft VPN.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix H, it is respectfully asserted that each of the limitations of claims 10 and 12 - 15 is fully disclosed by the Microsoft VPN reference, which therefore anticipates each of claims 10 and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Microsoft

VPN reference discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, the Microsoft VPN discloses the well-known use of computer memory to store information at least at pages 11, 15, and 16. Computer-readable instructions correspond to the software performing the functions disclosed in the reference. See Microsoft VPN at pages 11 and 37. Accordingly, the Microsoft VPN reference anticipates each of the limitations of claim 17.

Claims 26 and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in the Microsoft VPN, as shown in Appendix H. The limitations recited in claims 26 and 28 - 31 map closely to the limitations recited in claims 10 and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 10 and 12 - 15, and based upon the citations presented in Appendix H, it is respectfully asserted that each of the limitations of claims 26 and 28 - 31 is fully disclosed in the Microsoft VPN reference, which therefore anticipates each of claims 26 and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Microsoft VPN discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, the Microsoft VPN reference discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Microsoft VPN at pages 11, 27, 28, 34, and 37. Accordingly, the Microsoft VPN reference anticipates the limitations of claim 33.

For the reasons presented above, it is respectfully submitted that each of claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Microsoft VPN prior art reference.

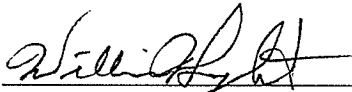
Summary

The new, non-cumulative prior art documents referred to above were not considered by the Examiner during prosecution of the '180 patent application. Since each of the limitations of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent is disclosed in these documents, contrary to the statement of reasons for allowance, a substantial new question of patentability is raised. Accordingly, the Requestor respectfully asks that this Request for *Inter Partes* Reexamination be granted and that the claims of the '180 patent be reexamined in view of the prior art presented herein.

If any fees are required in connection with this Request, please charge the same to our Deposit Account No. 02-2135.

Respectfully submitted,

ROTHWELL, FIGG, ERNST & MANBECK, P.C.

By: 
William N. Hugnet
Reg. No. 44,481

Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street, NW
Suite 800
Washington, D.C. 20005
Telephone: (202) 626-3534
Facsimile: (202) 783-6031

Date: December 8, 2009

CERTIFICATE OF SERVICE

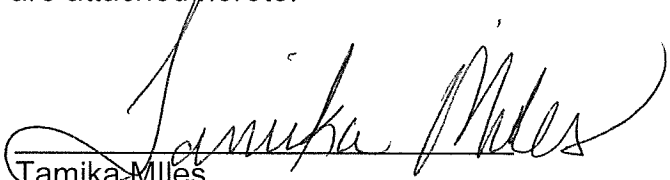
I hereby certify that true and correct copies of the **Replacement Request for Inter Partes Reexamination of Patent**, were served via Federal Express, by the undersigned, on **December 8, 2009**, to:

VirnetX, Inc.
c/o Banner & Witcoff, Ltd.
1100 13th Street, N.W., Suite 1200
Washington, D.C. 20005-4051

&

VirnetX, Inc.
5615 Scotts Valley Drive, Suite 110
Scotts Valley, CA 95066

A copy of the Federal Express Receipts are attached hereto.


Tamika Miles

From: Origin ID: JPNA (202) 626-3565
Tamika Miles
Rothwell, Figg, Ernst
1425 K Street, N.W.
Suite 800
Washington, DC 20005



J09300907312023

Ship Date: 08DEC09
ActWgt: 1.0 LB
CAD: 1139317/NET9090
Account#: S *****

Delivery Address Bar Code



Ref # 3755-180
Invoice #
PO #
Dept #

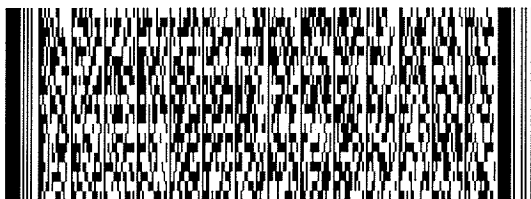
SHIP TO: (831) 438-8200 BILL SENDER

VirnetX, Inc.
5615 SCOTTS VALLEY DR STE 110
SCOTTS VALLEY, CA 95066

WED - 09DEC A5

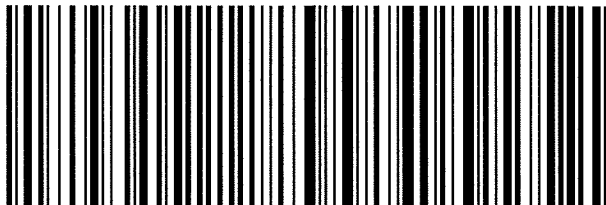
TRK# 7982 0381 2579
0201

PRIORITY OVERNIGHT



95066
CA-US
SJC

XX SRUA



After printing this label:

1. Use the 'Print' button on this page to print your label to your laser or inkjet printer.
2. Fold the printed page along the horizontal line.
3. Place label in shipping pouch and affix it to your shipment so that the barcode portion of the label can be read and scanned.

Warning: Use only the printed original label for shipping. Using a photocopy of this label for shipping purposes is fraudulent and could result in additional billing charges, along with the cancellation of your FedEx account number.

Use of this system constitutes your agreement to the service conditions in the current FedEx Service Guide, available on fedex.com. FedEx will not be responsible for any claim in excess of \$100 per package, whether the result of loss, damage, delay, non-delivery, misdelivery, or misinformation, unless you declare a higher value, pay an additional charge, document your actual loss and file a timely claim. Limitations found in the current FedEx Service Guide apply. Your right to recover from FedEx for any loss, including intrinsic value of the package, loss of sales, income interest, profit, attorney's fees, costs, and other forms of damage whether direct, incidental, consequential, or special is limited to the greater of \$100 or the authorized declared value. Recovery cannot exceed actual documented loss. Maximum for items of extraordinary value is \$500, e.g. jewelry, precious metals, negotiable instruments and other items listed in our Service Guide. Written claims must be filed within strict time limits, see current FedEx Service Guide.

Electronic Acknowledgement Receipt

EFS ID:	6596968
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	22907
Filer:	William Neal Hughet/Tamika Miles
Filer Authorized By:	William Neal Hughet
Attorney Docket Number:	3755-121
Receipt Date:	08-DEC-2009
Filing Date:	
Time Stamp:	17:50:09
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Receipt of Corrected Original Inter Partes Request	ReplacementRequestforInterPartesReexam180.pdf	3576452 <small>8547edae3cba1350b2708a3475582d3721621db6</small>	no	57

Warnings:

Information:

2	Reexam Certificate of Service	CertificateofServicefor180.pdf	83560 fa499589dd2a5cc0e3c5b9d48bcf0541363f1766	no	2
---	-------------------------------	--------------------------------	---------------------------------------------------	----	---

Warnings:

Information:

Total Files Size (in bytes):	3660012
-------------------------------------	---------

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

New Applications Under 35 U.S.C. 111


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


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

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

New International Application Filed with the USPTO as a Receiving Office

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

<i>Application Number</i> 	Application/Control No. 95/001,270	Applicant(s)/Patent Under Reexamination 7188180
	Examiner	Art Unit 3999

Index of Claims 	Application/Control No. 95001270	Applicant(s)/Patent Under Reexamination 7188180
	Examiner	Art Unit 3999

✓	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										
	41										

Issue Classification



Application/Control No.
95001270

Applicant(s)/Patent Under Reexamination
7188180

Examiner


Art Unit
3999

ORIGINAL						INTERNATIONAL CLASSIFICATION											
CLASS			SUBCLASS			CLAIMED					NON-CLAIMED						
709			227														
CROSS REFERENCE(S)																	
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

(Assistant Examiner) _____ (Date) _____		Total Claims Allowed:	
		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner) _____ (Date) _____			


Reexamination 	Application/Control No. 95001270	Applicant(s)/Patent Under Reexamination 7188180
	Certificate Date	Certificate Number

Requester Correspondence Address:	<input type="checkbox"/> Patent Owner	<input checked="" type="checkbox"/> Third Party
ROTHWELL, FIGG, RENST & MANBECK, P.C. 1425 K STREET N.W. SUITE 800 WASHINGTON, D.C. 20005		

LITIGATION REVIEW <input type="checkbox"/>	(examiner initials)	(date)
Case Name	Director Initials	

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

--	--

Search Notes 	Application/Control No. 95001270	Applicant(s)/Patent Under Reexamination 7188180
	Examiner	Art Unit 3999

SEARCHED			
Class	Subclass	Date	Examiner
709	227		

SEARCH NOTES		
Search Notes	Date	Examiner

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--



UNITED STATES PATENT AND TRADEMARK OFFICE

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



Bib Data Sheet

CONFIRMATION NO. 2128

SERIAL NUMBER 95/001,270	FILING OR 371(c) DATE 12/08/2009 RULE	CLASS 709	GROUP ART UNIT 3992	ATTORNEY DOCKET NO. 3755-121
------------------------------------	-----------------------------------------------------------	---------------------	-------------------------------	----------------------------------------

APPLICANTS
 7188180, Residence Not Provided;
 VIRNETX INC.(OWNER), SCOTTSVALLEY DRIVE, CA;
 MICROSOFT CORPORATION(3RD. PTY. REQ.), CHEVY CHASE, MD;
 MICROSOFT CORPORATION(REAL PTY. IN INTEREST), CHEVY CHASE, MD;
 ROTHWELL, FIGG, ERNST & MANBECK, P.C., WASHINGTON, DC

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

**** FOREIGN APPLICATIONS *******

Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after Allowance				
Verified and Acknowledged	Examiner's Signature	Initials		

ADDRESS
 22907

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

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	<input type="checkbox"/> All Fees
		<input type="checkbox"/> 1.16 Fees (Filing)
		<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)
		<input type="checkbox"/> 1.18 Fees (Issue)
		<input type="checkbox"/> Other _____
		<input type="checkbox"/> Credit

Patent Assignment Abstract of Title

Total Assignments: 2

Application #: 10702486

Filing Dt: 11/07/2003

Patent #: 7188180

Issue Dt: 03/06/2007

PCT #: NONE

Publication #: US20040107285

Pub Dt: 06/03/2004

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

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

Assignment: 1

Reel/Frame: 014679 / 0947

Received: 11/14/2003

Recorded: 11/07/2003

Mailed: 06/03/2004

Pages: 3

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors: LARSON, VICTOR

Exec Dt: 11/06/2003

SHORT, ROBERT DUNHAM III

Exec Dt: 10/27/2003

MUNGER, EDMUND COLBY

Exec Dt: 11/05/2003

WILLIAMSON, MICHAEL

Exec Dt: 11/05/2003

Assignee: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

10260 CAMPUS POINT DRIVE

SAN DIEGO, CALIFORNIA 92121

Correspondent: BANNER & WITCOFF, LTD.

ROSS A. DANNENBERG

1001 G STREET, N.W., 11TH FLOOR

WASHINGTON, DC 20001

Assignment: 2

Reel/Frame: 018757 / 0326

Received: 01/10/2007

Recorded: 01/10/2007

Mailed: 01/16/2007

Pages: 5

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

Exec Dt: 12/21/2006

Assignee: VIRNETX INC.

5615 SCOTTS VALLEY DRIVE, SUITE 110

SCOTTS VALLEY DRIVE, CALIFORNIA 95066

Correspondent: BANNER & WITCOFF, LTD.

1001 G STREET, N.W. - 11TH FLOOR

WASHINGTON, D.C. 20001-4597

Search Results as of: 12/09/2009 04:19 PM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350.
Web interface last modified: October 18, 2008 v.2.0.1

Litigation Search Report CRU 3999

Reexam Control No. 95/001,270

TO: MARK REINHART
Location: CRU
Art Unit: 3992
Date: 12/09/09

From: MANUEL SALDANA
Location: CRU 3999
MDW 7C55
Phone: (571) 272-7740

MANUEL.SALDANA@uspto.gov

Search Notes

Litigation was NOT found for US Patent Number: 7,188,180.

- 1) I performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.
- 2) I performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.
- 3) I performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.
- 4) I performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.
- 5) I performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

KEYCITE

C US PAT 7188180 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, Assignee: VimetX, Inc. (Mar 06, 2007)

History**Direct History**

- => 1 **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**, US PAT 7188180, 2007 WL 665444 (U.S. PTO Utility Mar 06, 2007) (NO. 10/702486)

Patent Family

- 2 **INFORMATION TRANSMISSION INVOLVES COMPARING DISCRIMINATOR VALUE FOR EACH RECEIVED DATA PACKET WITH SET OF VALID DISCRIMINATOR VALUES, ACCEPTING RECEIVED DATA PACKET FOR FURTHER PROCESSING WHILE DETECTING MATCH**, Derwent World Patents Legal 2000-399393

Assignments

- 3 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS). Number of Pages: 005, (DATE RECORDED: Jan 10, 2007)
 4 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS). Number of Pages: 003, (DATE RECORDED: Nov 07, 2003)

Patent Status Files

- .. Certificate of Correction, (OG DATE: Aug 28, 2007)

Prior Art (Coverage Begins 1976)

- C** 6 **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY**, US PAT 7010604 Assignee: Science Applications International, (U.S. PTO Utility 2006)
C 7 **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY**, US PAT 6502135 Assignee: Science Applications International, (U.S. PTO Utility 2002)
C 8 **APPARATUS AND METHOD FOR ESTABLISHING A CRYPTOGRAPHIC LINK BETWEEN ELEMENTS OF A SYSTEM**; US PAT 5787172 Assignee: The Merdan Group, Inc., (U.S. PTO Utility 1998)
C 9 **AUTOCONFIGURABLE METHOD AND SYSTEM HAVING AUTOMATED DOWNLOADING**, US PAT 5870610 Assignee: Siemens Business Communication Systems,, (U.S. PTO Utility

- 1999)
- C** 10 CRYPTOGRAPHIC KEY MANAGEMENT APPARATUS AND METHOD, US PAT 5341426 Assignee: Motorola, Inc., (U.S. PTO Utility 1994)
 - C** 11 DOMAIN NAME ROUTING, US PAT 6119171 Assignee: IP Dynamics, Inc., (U.S. PTO Utility 2000)
 - C** 12 DOMAIN NAME SYSTEM LOOKUP ALLOWING INTELLIGENT CORRECTION OF SEARCHES AND PRESENTATION OF AUXILIARY INFORMATION, US PAT 6332158 (U.S. PTO Utility 2001)
 - C** 13 DYNAMIC NETWORK ADDRESS UPDATING, US PAT 6243749 Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2001)
 - C** 14 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 6052788 Assignee: Network Engineering Software, Inc., (U.S. PTO Utility 2000)
 - C** 15 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 5898830 Assignee: Network Engineering Software, (U.S. PTO Utility 1999)
 - C** 16 MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS, US PAT 5905859 Assignee: International Business Machines, (U.S. PTO Utility 1999)
 - C** 17 METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION, US PAT 5796942 Assignee: Computer Associates International, Inc., (U.S. PTO Utility 1998)
 - C** 18 METHOD AND APPARATUS FOR CLIENT-HOST COMMUNICATION OVER A COMPUTER NETWORK, US PAT 6119234 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 2000)
 - C** 19 METHOD AND APPARATUS FOR CONFIGURING A VIRTUAL PRIVATE NETWORK, US PAT 6226751 Assignee: VPN Technologies, Inc., (U.S. PTO Utility 2001)
 - C** 20 METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM, US PAT 5892903 Assignee: Internet Security Systems, Inc., (U.S. PTO Utility 1999)
 - C** 21 METHOD AND APPARATUS FOR AN INTERNET PROTOCOL (IP) NETWORK CLUSTERING SYSTEM, US PAT 6006259 Assignee: Network Alchemy, Inc., (U.S. PTO Utility 1999)
 - C** 22 METHOD AND APPARATUS FOR A KEY-MANAGEMENT SCHEME FOR INTERNET PROTOCOLS, US PAT 5588060 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1996)
 - C** 23 METHOD AND APPARATUS FOR MANAGING A VIRTUAL PRIVATE NETWORK, US PAT 6079020 Assignee: VPN Technologies, Inc., (U.S. PTO Utility 2000)
 - C** 24 METHOD AND APPARATUS FOR PROVIDING NETWORK ACCESS CONTROL USING A DOMAIN NAME SYSTEM, US PAT 6256671 Assignee: Nortel Networks Limited, (U.S. PTO Utility 2001)
 - C** 25 METHOD AND APPARATUS FOR PROVIDING A VIRTUAL PRIVATE NETWORK, US PAT 6092200 Assignee: Novell, Inc., (U.S. PTO Utility 2000)
 - C** 26 METHOD AND PROTOCOL FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION, US PAT 6353614 Assignee: 3Com Corporation, (U.S. PTO Utility 2002)

© 2009 Thomson Reuters. All rights reserved.

- C** 27 METHOD AND SYSTEM FOR AUTOMATIC DISCOVERY OF NETWORK SERVICES, US PAT 6286047 Assignee: Hewlett-Packard Company, (U.S. PTO Utility 2001)
- C** 28 MULTI-ACCESS VIRTUAL PRIVATE NETWORK, US PAT 6158011 Assignee: V-One Corporation, (U.S. PTO Utility 2000)
- C** 29 NETWORK COMMUNICATIONS ADAPTER WITH DUAL INTERLEAVED MEMORY BANKS SERVICING MULTIPLE PROCESSORS, US PAT 4933846 Assignee: Network Systems Corporation, (U.S. PTO Utility 1990)
- C** 30 NETWORK WITH SECURE COMMUNICATIONS SESSIONS, US PAT 5689566 (U.S. PTO Utility 1997)
- H** 31 POLICY CACHING METHOD AND APPARATUS FOR USE IN A COMMUNICATION DEVICE BASED ON CONTENTS OF ONE DATA UNIT IN A SUBSET OF RELATED DATA UNITS, US PAT 5842040 Assignee: Storage Technology Corporation, (U.S. PTO Utility 1998)
- C** 32 SECURE DELIVERY OF INFORMATION IN A NETWORK, US PAT 6178505 Assignee: Internet Dynamics, Inc., (U.S. PTO Utility 2001)
- C** 33 SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY, US PAT 5805801 Assignee: International Business Machines, (U.S. PTO Utility 1998)
- C** 34 SYSTEM AND METHOD FOR MANAGING SECURITY OBJECTS, US PAT 6330562 Assignee: International Business Machines, (U.S. PTO Utility 2001)
- C** 35 SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE, US PAT 5878231 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1999)
- C** 36 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR MULTIPLE-ENTRY POINT VIRTUAL POINT OF SALE ARCHITECTURE, US PAT 6178409 Assignee: VeriFone, Inc., (U.S. PTO Utility 2001)
- C** 37 VIRTUAL PRIVATE NETWORK SYSTEM OVER PUBLIC MOBILE DATA NETWORK AND VIRTUAL LAN, US PAT 6016318 Assignee: NEC Corporation, (U.S. PTO Utility 2000)

Single Search - with Terms and Connectors

Enter keywords - Search multiple dockets & documents

Search

[View Demo](#)
[Search Tips](#)

[My CourtLink](#)

[Search](#)

[Dockets & Documents](#)

[Track](#)

[Alert](#)

[Strategic Profiles](#)

[My Account](#)



[Search](#) > [Patent Search](#) > [Searching](#)

Patent Search 7188180 12/9/2009

No cases found.

[Return to Search](#)

(Charges for search still apply)



[About LexisNexis](#) | [Terms & Conditions](#) | [Pricing](#) | [Privacy](#) | [Customer Support](#) - 1-888-311-1966
Copyright © 2009 LexisNexis®. All rights reserved.

Legal > / ... / > Utility, Design and Plant Patents ⓘ

Search ⓘ

Select Search Type and Enter Search Terms

Terms & Connectors	PATNO= 7188180
Natural Language	
Easy Search™	
Semantic Search	
What's this?	

[Suggest terms for my search](#)

Search

[Check spelling](#)

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment Add

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions From To Date formats...

Search Connectors

- and and w/p in same paragraph
- or or w/seg in same segment
- w/N within N words w/s in same sentence
- pre/N precedes by N words and not and not

> [More Connectors & Commands...](#)

How Do I...?

- > [Combine sources?](#)
- > [Restrict by date?](#)
- > [Restrict by document segment?](#)
- > [Use wildcards as placeholders for one or more characters in a search term?](#)

[View Tutorials](#)



Source: [Legal > / ... / > Utility, Design and Plant Patents](#) Terms: **PATNO= 7188180** ([Edit Search](#) | [Suggest Terms for My Search](#))

702486 (10) 7188180 March 6, 2007 ,

UNITED STATES PATENT AND TRADEMARK OFFICE GRANTED PATENT

7188180[Get Drawing Sheet 1 of 40](#)[Access PDF of Official Patent *](#)[Order Patent File History / Wrapper from REEDFAX®](#)[Link to Claims Section](#)

June 3, 2004 ,

Method for establishing secure communication link between computers of virtual private network

INVENTOR: Larson, Victor - Fairfax, VIRGINIA , , United States of America (US) ; Short, III, Robert Durham - Leesburg, VIRGINIA , , United States of America (US) ; Munger, Edmund Colby - Crownsville, MARYLAND , , United States of America (US) ; Williamson, Michael - South Riding, VIRGINIA , , United States of America (US)

APPL-NO: 702486 (10)**FILED-DATE:** November 7, 2003**GRANTED-DATE:** March 6, 2007 ,**CORE TERMS:** packet, computer, server, network, message, router, sync, node, transmitter, receiver ...**ENGLISH-ABST:**

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

Source: [Legal > / ... / > Utility, Design and Plant Patents](#) Terms: **PATNO= 7188180** ([Edit Search](#) | [Suggest Terms for My Search](#))

View: KWIC

Date/Time: Wednesday, December 9, 2009 - 4:38 PM EST

Legal > / ... / > Patent Cases from Federal Courts and Administrative Materials ⓘ

Search ⓘ

Select Search Type and Enter Search Terms

Terms & Connectors	7188180 OR 7,188,180
Natural Language	
Easy Search™	

Suggest terms for my search

Search

Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment Add ↑

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions From To Date formats...

Search Connectors

- and and w/p in same paragraph
- or or w/seg in same segment
- w/N within N words w/s in same sentence
- pre/N precedes by N words and not and not

> [More Connectors & Commands...](#)

How Do I...?

- > [Combine sources?](#)
- > [Restrict by date?](#)
- > [Restrict by document segment?](#)
- > [Use wildcards as placeholders for one or more characters in a search term?](#)

[View Tutorials](#)



Source: [Legal](#) > / ... / > Patent Cases from Federal Courts and Administrative Materials ⓘTerms: 7188180 OR 7,188,180 ([Edit Search](#) | [Suggest Terms for My Search](#))

☛ Select for FOCUS™ or Delivery

- ⓘ 1. [VirnetX, Inc. v. Microsoft Corp.](#), CASE NO. 6:07 CV 80, UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS, TYLER DIVISION, 2009 U.S. Dist. LEXIS 65667, July 30, 2009, Decided, July 30, 2009, Filed

CORE TERMS: network, domain, web, virtual, site, specification, server, user, target, proxy ...

- ⓘ 2. [VirnetX, Inc. v. Microsoft Corp.](#), CASE NO. 6:07 CV 80, UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS, TYLER DIVISION, 2008 U.S. Dist. LEXIS 94854, June 3, 2008, Decided, June 4, 2008, Filed, Patent interpreted by VirnetX, Inc. v. Microsoft Corp., 2009 U.S. Dist. LEXIS 65667 (E.D. Tex., July 30, 2009)

CORE TERMS: patent-in-suit, patent, license, infringement, grantor, patent rights, substantial rights, grantee, joinder, join ...Source: [Legal](#) > / ... / > Patent Cases from Federal Courts and Administrative Materials ⓘTerms: 7188180 OR 7,188,180 ([Edit Search](#) | [Suggest Terms for My Search](#))

View: Cite

Date/Time: Wednesday, December 9, 2009 - 4:38 PM EST

* Signal Legend:

- - Warning: Negative treatment is indicated
- Ⓚ - Questioned: Validity questioned by citing refs
- ⚠ - Caution: Possible negative treatment
- ⊕ - Positive treatment is indicated
- Ⓐ - Citing Refs. With Analysis Available
- Ⓘ - Citation information available

* Click on any Shepard's signal to Shepardize® that case.

Legal > / . . . / > Patent, Trademark & Copyright Periodicals, Combined ⓘ

Search ⓘ

Select Search Type and Enter Search Terms

Terms & Connectors	7188180 OR 7,188,180
Natural Language	
Easy Search™	

[Suggest terms for my search](#)

Search

[Check spelling](#)

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment Add

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions From To Date formats...

Search Connectors

- and and w/p in same paragraph
- or or w/seg in same segment
- w/N within N words w/s in same sentence
- pre/N precedes by N words and not and not

> [More Connectors & Commands...](#)

How Do I...?

- > [Combine sources?](#)
- > [Restrict by date?](#)
- > [Restrict by document segment?](#)
- > [Use wildcards as placeholders for one or more characters in a search term?](#)

[View Tutorials](#)



No Documents Found

No documents were found for your search terms

"7188180 OR 7,188,180"

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -

Click "Edit Search" to return to the search form and modify your search.

Suggestions:

- Check for spelling errors .
 - Remove some search terms.
 - Use more common search terms, such as those listed in "Suggested Words and Concepts"
 - Use a less restrictive date range.
-

Save this Search as an Alert

Edit Search



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)
Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

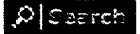
Legal > /... / > News, All (English, Full Text) ?

Search

Select Search Type and Enter Search Terms

Terms & Connectors	7188180 OR 7,188,180
Natural Language	
Easy Search™	

Suggest terms for my search



Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment Add ↑

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions From To Date formats...

Search Connectors

- and and w/p in same paragraph
- or or w/seg in same segment
- w/N within N words w/s in same sentence
- pre/N precedes by N words and not and not

> More Connectors & Commands...

How Do I...?

- > Combine sources?
- > Restrict by date?
- > Restrict by document segment?
- > Use wildcards as placeholders for one or more characters in a search term?

View Tutorials



Source: [Legal](#) > / ... / > **News, All (English, Full Text)** ⓘ

Terms: **7188180 OR 7,188,180** ([Edit Search](#) | [Suggest Terms for My Search](#))

↙ Select for FOCUS™ or Delivery

- 1. [Virginia, Maryland Inventors Develop Secure Computer Network Address Access Method](#), US Fed News, March 19, 2007 Monday 11:41 PM EST, , 293 words, US Fed News, Alexandria, Va.
- 2. [Third Quarter Free Cash Flow Turns Negative for AMCON](#), Cashflow news, November 30, 2006 Thursday 6:02 PM EST, , 286 words

Source: [Legal](#) > / ... / > **News, All (English, Full Text)** ⓘ

Terms: **7188180 OR 7,188,180** ([Edit Search](#) | [Suggest Terms for My Search](#))

View: Cite

Date/Time: Wednesday, December 9, 2009 - 4:38 PM EST





UNITED STATES PATENT AND TRADEMARK OFFICE

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

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/001,270	12/08/2009	7188180

**CONFIRMATION NO. 2128
ASSIGNMENT NOTICE**

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051



Date Mailed: 12/10/2009

NOTICE OF ASSIGNMENT OF *INTER PARTES* REEXAMINATION REQUEST

The above-identified request for *inter partes* reexamination has been assigned to Art Unit 3992. All future correspondence in this proceeding should be identified by the control number listed above and directed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or, if none is of record, to all owners of record. (See 37 CFR 1.33(c).) If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s)

(MPEP 2222). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned with the request to withdraw pursuant to Section 1.36.

cc: Third Party Requester
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, DC 20005

/sdstevenson/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900



UNITED STATES PATENT AND TRADEMARK OFFICE

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

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/001,270	12/08/2009	7188180

ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, DC 20005

CONFIRMATION NO. 2128
REEXAM ASSIGNMENT NOTICE



Date Mailed: 12/10/2009

NOTICE OF *INTER PARTES* REEXAMINATION REQUEST FILING DATE

Requester is hereby notified that the filing date of the request for *inter partes* reexamination is 12/08/2009, the date that the filing requirements of 37 CFR § 1.915 were received.

A decision on the request for *inter partes* reexamination will be mailed within three months from the filing date of the request for *inter partes* reexamination. (See 37 CFR 1.923.)

A copy of this Notice is being sent to the person identified by the requestor as the patent owner. Further patent owner correspondence will be with the latest attorney or agent of record in the patent file. (See 37 CFR 1.33.) Any paper filed should include a reference to the present request for *inter partes* reexamination (by Reexamination Control Number) and should be addressed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

cc: Patent Owner
22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

/sdstevenson/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900



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

95/001,270 12/08/2009 7188180 3755-121 2128

22907 7590 01/19/2010
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER

NALVEN, ANDREW L

ART UNIT PAPER NUMBER

3992

MAIL DATE DELIVERY MODE

01/19/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, D.C. 20005

MAILED
Date: **JAN 19 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)

**ORDER GRANTING/DENYING
REQUEST FOR INTER PARTES
REEXAMINATION**

Control No.	Patent Under Reexamination	
95/001,270	7188180	
Examiner	Art Unit	
ANDREW L. NALVEN	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

The request for *inter partes* reexamination has been considered. Identification of the claims, the references relied on, and the rationale supporting the determination are attached.

Attachment(s): PTO-892 PTO/SB/08 Other: Decision on Request

1. The request for *inter partes* reexamination is GRANTED.

An Office action is attached with this order.

An Office action will follow in due course.

2. The request for *inter partes* reexamination is DENIED.

This decision is not appealable. 35 U.S.C. 312(c). Requester may seek review of a denial by petition to the Director of the USPTO within ONE MONTH from the mailing date hereof. 37 CFR 1.927. EXTENSIONS OF TIME ONLY UNDER 37 CFR 1.183. In due course, a refund under 37 CFR 1.26(c) will be made to requester.

All correspondence relating to this *inter partes* reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Order.

DECISION GRANTING INTER PARTES REEXAMINATION

A substantial new question of patentability affecting claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of United States Patent Number 7,188,180 (hereafter "the '180 patent") is raised by the request for *inter partes* reexamination submitted on December 8, 2009.

Notification of Concurrent Proceedings

The patent owner is reminded of the continuing responsibility under 37 CFR 1.985 to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the '180 patent throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP § 2686 and 2686.04.

PROSECUTION HISTORY

The '180 patent was issued on March 6, 2007 from an application filed November 7, 2003. During the prosecution of the '180 patent, a notice of allowance was issued on November 12, 2006. The notice of allowance specified the reasons for allowance as the failure of the prior art to teach "requesting a secure computer network address from

Art Unit: 3992

a secure domain name server according to the secure domain name; and using a virtual private network communication link to send an access request message to the secure computer network address" (see prosecution history of application 10/702,486, Notice of Allowance mailed 11/12/2006).

PROPOSED SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Third Party Requester ("Requester") requested reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent based upon the following prior art patents and publications:

1. Aventail Administrator's Guide (hereafter "Aventail") that was published between 1996 and 1999. Aventail was not considered in a prior examination and qualifies as prior art under §102(a).
2. Microsoft Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview") that was published in 1998. VPN Overview was not considered in a prior examination and qualifies as prior art under §102(b).
3. RFC 1035 that was published in 1987. RFC 1035 was not considered in a prior examination and qualifies as prior art under §102(b).
4. "Building and Managing Virtual Private Networks" that was published by David Kosiur in 1998 (hereafter "Kosiur"). Kosiur was not considered in a prior examination and qualifies as prior art under §102(b).

5. "Implementing IPsec" that was published by Elizabeth Kaufman on September 7, 1999 (hereafter "Kaufman." Kaufman was not considered in a prior examination and qualifies as prior art under §102(a).
6. "Public Key Distribution with Secure DNS" by James Galvin that was published in July 1996 (hereafter "Galvin"). Galvin was not considered during a prior examination and qualifies as prior art under §102(b).
7. Gauntlet Firewall for Windows NT, Administrator's Guide (hereafter "Gauntlet") that was published no later than 1999. Gauntlet was not considered in a prior examination and qualifies as prior art under §102(a).
8. Microsoft Windows NT Technical Support: Hands-On, Self-paced Training for Support Version 4.0 (hereafter "Hands-On"). Hands-On was published in 1998 and qualifies as prior art under §102(b). Hands-On was not considered in a prior examination.
9. Microsoft Windows NT Sever, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Severs (hereafter "Installing NT"). Installing NT was published in 1997 and qualifies as prior art under §102(b). Installing NT was not considered in a prior examination.
10. Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources (hereafter "Microsoft VPN") that was published on January 1, 2000. Microsoft VPN was not considered in a prior examination and qualifies as prior art under §102(a).

Requestor has alleged a substantial new question of patentability in light of the proposed rejections:

Issue 1 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Aventail under 35 U.S.C. §102(a).

Issue 2 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of VPN Overview in view of RFC 1035 under 35 U.S.C. 103(a).

Issue 3 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kosiur under 35 U.S.C. §102(b).

Issue 4 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kaufman under 35 U.S.C. §102(a).

Issue 5 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Kaufman in view of Galvin under 35 U.S.C. 103(a).

Issue 6 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Gauntlet under 35 U.S.C. §102(a).

Issue 7 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Hands-On in view of Installing NT under 35 U.S.C. 103(a).

Issue 8 - Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are anticipated by Microsoft VPN under 35 U.S.C. §102(a).

ANALYSIS OF SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Summary

Requestor has shown a substantial new question of patentability with regards to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35.

Analysis

A substantial new question of patentability is raised by a cited patent or printed publication when there is a substantial likelihood that a reasonable examiner would consider the prior art patent or printed publication important in deciding whether or not the claim is patentable. A substantial new question of patentability is not raised by prior art presented in a reexamination request if the Office has previously considered (in an earlier examination of the patent) the same question of patentability as to a patent claim favorable to the patent owner based on the same prior art patents or printed publications. In re Recreative Technologies, 83 F.3d 1394, 38 USPQ2d 1776 (Fed. Cir. 1996).

Aventail Reference

Aventail raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 1. Aventail raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Aventail at least discloses requesting a secure computer network address from a secure domain name server according to the secure domain name (Aventail, page 11, the application does a DNS lookup). Aventail's DNS request seeks a "secure" computer network address because Aventail discloses the listing of domain names associated with a redirection rule. These special domains require the proxying of traffic (Aventail, page 11). When proxying the traffic to the secure computer network address, Aventail executes authentication processing (Aventail, page 11) and in some cases transmits and receives data using encryption (Aventail, page 12).

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Aventail important in deciding whether or not the claims are patentable. Accordingly, Aventail raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

VPN Overview Reference

VPN Overview raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 2. VPN Overview raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

Art Unit: 3992

For example, VPN Overview at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (VPN Overview, page 9 – gain access to the protected resources). VPN Overview discloses an access request message by disclosing that a client gains access to protected resources of a corporate hub (VPN Overview, page 9). This necessarily implies that the client is requesting access to some particular resource. The requests for access are transmitted through the established VPN in order to ensure that only those users with proper credentials can gain access to the protected resources.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider VPN Overview important in deciding whether or not the claims are patentable. Accordingly, VPN Overview raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Kosiur Reference

Kosiur raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 3. Kosiur raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

Art Unit: 3992

For example, Kosiur at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Kosiur, pages 40-42). Kosiur discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection. By accessing information over a VPN, Kosiur requires the sending of an access request message.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Kosiur important in deciding whether or not the claims are patentable. Accordingly, Kosiur raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Kaufman Reference

Kaufman raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issues 4 and 5. Kaufman raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Kaufman at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Kaufman, Pages 65, 94, and 141). Kaufman discloses the limitation by teaching

Art Unit: 3992

that a VPN connection is used to securely connect to a remote device in order to access content (Kaufman, Pages 65 and 141).

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Kaufman important in deciding whether or not the claims are patentable. Accordingly, Kaufman raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Gauntlet Reference

Gauntlet raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 6. Gauntlet raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Gauntlet at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Gauntlet, Section 18-1, client can connect through PPTP to read mail or access other internal data). Gauntlet discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection which suggests that there must be a request for information.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Gauntlet important in deciding whether or not the claims are patentable. Accordingly, Gauntlet raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Hands-On Reference

Hands-On raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 7. Hands-On raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Hands-On at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Hands-On, Page 431, remotely access corporate network). Hands-On discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection which suggests that there must be a request for information.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a

Art Unit: 3992

reasonable examiner would consider Hands-On important in deciding whether or not the claims are patentable. Accordingly, Hands-On raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Microsoft VPN Reference

Microsoft VPN raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, and 28-31 as presented in Issue 8. Microsoft VPN raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Microsoft VPN at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Microsoft VPN, Pages 11-12, remote access to an organization server). Microsoft VPN discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection which suggests that there must be a request for information.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Microsoft VPN important in deciding whether or not the claims are patentable. Accordingly, Microsoft VPN raises a substantial new

Art Unit: 3992

question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, and 28-31 that has not been decided in a previous examination.

CORRESPONDENCE

All correspondence relating to this inter partes reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at <https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html>.

By Mail to: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

For EFS-Web transmissions, 37 CFR 1.8(a)(1)(i) (C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) includes a

Art Unit: 3992

certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication or earlier communications from the Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: ASK



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,270	12/08/2009	7188180	3755-121	2128

22907 7590 01/19/2010
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
01/19/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

OFFICE ACTION IN INTER PARTES REEXAMINATION	Control No.	Patent Under Reexamination	
	95/001,270	7188180	
	Examiner	Art Unit	
	ANDREW L. NALVEN	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:

Patent Owner on _____

Third Party(ies) on 8 December 2009

RESPONSE TIMES ARE SET TO EXPIRE AS FOLLOWS:

For Patent Owner's Response:

2 MONTH(S) from the mailing date of this action. 37 CFR 1.945. EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.956.

For Third Party Requester's Comments on the Patent Owner Response:

30 DAYS from the date of service of any patent owner's response. 37 CFR 1.947. NO EXTENSIONS OF TIME ARE PERMITTED. 35 U.S.C. 314(b)(2).

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

This action is not an Action Closing Prosecution under 37 CFR 1.949, nor is it a Right of Appeal Notice under 37 CFR 1.953.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. Notice of References Cited by Examiner, PTO-892
2. Information Disclosure Citation, PTO/SB/08
3. _____

PART II. SUMMARY OF ACTION:

- 1a. Claims 1,4,10,12-15,17,20,26,28-31,33 and 35 are subject to reexamination.
- 1b. Claims 2, 3, 5-9, 11, 16, 18,19, 21-25, 27, 32, 34, 36-41 are not subject to reexamination.
2. Claims _____ have been canceled.
3. Claims 4,20,35 are confirmed. [Unamended patent claims] ^{ESC}
4. Claims _____ are patentable. [Amended or new claims]
5. Claims 1, 10,12-15,17,26,28-31,33 are rejected.
6. Claims 4,20 and 35 are objected to. ^{ESC}
7. The drawings filed on _____ are acceptable are not acceptable.
8. The drawing correction request filed on _____ is: approved. disapproved.
9. Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has:
 been received. not been received. been filed in Application/Control No 95001270.
10. Other _____

Inter Partes Reexamination Office Action

Third Party Requester ("Requester") requested reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of United States Patent Number 7,188,180 (hereafter "the '180 patent") issued to Larson et al based upon the following prior art patents and publications:

1. Aventail Administrator's Guide (hereafter "Aventail") that was published between 1996 and 1999. Aventail was not considered in a prior examination and qualifies as prior art under §102(a).
2. Microsoft Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview") that was published in 1998. VPN Overview was not considered in a prior examination and qualifies as prior art under §102(b).
3. RFC 1035 that was published in 1987. RFC 1035 was not considered in a prior examination and qualifies as prior art under §102(b).
4. "Building and Managing Virtual Private Networks" that was published by David Kosiur in 1998 (hereafter "Kosiur"). Kosiur was not considered in a prior examination and qualifies as prior art under §102(b).
5. "Implementing IPsec" that was published by Elizabeth Kaufman on September 7, 1999 (hereafter "Kaufman." Kaufman was not considered in a prior examination and qualifies as prior art under §102(a).

Art Unit: 3992

6. "Public Key Distribution with Secure DNS" by James Galvin that was published in July 1996 (hereafter "Galvin"). Galvin was not considered during a prior examination and qualifies as prior art under §102(b).
7. Gauntlet Firewall for Windows NT, Administrator's Guide (hereafter "Gauntlet") that was published no later than 1999. Gauntlet was not considered in a prior examination and qualifies as prior art under §102(a).
8. Microsoft Windows NT Technical Support: Hands-On, Self-paced Training for Support Version 4.0 (hereafter "Hands-On"). Hands-On was published in 1998 and qualifies as prior art under §102(b). Hands-On was not considered in a prior examination.
9. Microsoft Windows NT Sever, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers (hereafter "Installing NT"). Installing NT was published in 1997 and qualifies as prior art under §102(b). Installing NT was not considered in a prior examination.
10. Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources (hereafter "Microsoft VPN") that was published on January 1, 2000. Microsoft VPN was not considered in a prior examination and qualifies as prior art under §102(a).

The attached order granting reexamination found a substantial new question of patentability raised by the following proposed rejections:

Art Unit: 3992

Issue 1 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Aventail under 35 U.S.C. §102(a).

Issue 2 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of VPN Overview in view of RFC 1035 under 35 U.S.C. 103(a).

Issue 3 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kosiur under 35 U.S.C. §102(b).

Issue 4 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kaufman under 35 U.S.C. §102(a).

Issue 5 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Kaufman in view of Galvin under 35 U.S.C. 103(a).

Issue 6 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Gauntlet under 35 U.S.C. §102(a).

Issue 7 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Hands-On in view of Installing NT under 35 U.S.C. 103(a).

Issue 8 - Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are anticipated by Microsoft VPN under 35 U.S.C. §102(a).

Claim Rejections - 35 USC § 102 and 103

Art Unit: 3992

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Issue 1

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Aventail under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 are rejected under 35 U.S.C. 102(a) as being anticipated by Aventail. This rejection for claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 is adopted for the reasons set forth in the December 8,

Art Unit: 3992

2009 request for reexamination, on pages 12-19 and as presented in Appendix A, which is incorporated by reference. In addition, a rejection of claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 in view of Aventail is provided below which utilizes citations to Aventail provided in the request and additional citations provided by Examiner.

With regards to claim 1, Aventail teaches a method for accessing a secure computer network address (*Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Page 46 - SOCKS v5 servers often require user authentication before allowing access; Page 66 – To gain access to your extranet, users may need to traverse multiple firewalls...employee at a partner company...having an authenticated, encrypted, and controlled connection to your internal network*),

comprising steps of: receiving a secure domain name (*Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Pages 12-13 – if the requested domain name matches a redirection rule then it is part of a domain we are proxying traffic to – the domain name is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption; Examiner is interpreting the secure domain name as a domain name associated with a secure computer*);

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name (*Aventail, Page 12 - "If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a False DNS entry (HOSTENT) that it*

Art Unit: 3992

can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution," the SOCKS server acts to resolve/request the secure computer network address from a secure domain name service; Examiner is interpreting the query message as a DNS resolution request to a domain name server that can resolve addresses of secure computers);

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name (Aventail, Page 12 – "If the destination hostname matches a redirection rule...Aventail Connect will forward the hostname to the extranet SOCKS server and the SOCKS server performs the hostname resolution." Since the SOCKS server performs hostname resolution by requesting the secure computer network address, it is inherent that a message should be received that resolves the domain name to an address; Examiner is interpreting the response message as a DNS resolution message returning an address associated with a secure computer);

and sending an access request message to the secure computer network address using a virtual private network communication link (Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN; Examiner is interpreting the sending of the access request message as requesting access to a particular resource/content over a VPN).

Art Unit: 3992

With regards to claim 10, Aventail teaches the virtual private network includes the Internet (*Aventail, Page 5 – “Aventail...extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet”*).

With regards to claim 12, Aventail teaches the access request message contains a request for information stored at the secure computer network address (*Aventail, Page 77 – “The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.” – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN*).

With regards to claim 14, Aventail teaches the method of claim 1 performed by a software module (*Aventail, Page 7 – Aventail Connect is a client component. Aventail ExtraNet Server is a component that runs on a SOCKS 5 server; Page 9 – Aventail Connect is a layered service provider*).

With regards to claim 17, Aventail teaches a computer-readable storage medium, comprising: a storage area (*Aventail, Page 14 - Aventail Connect can be delivered on CD or as a network- delivered, self-extracting archive file; Page 15 - Aventail Connect can be installed to single workstation or to multiple networked workstations*);

and computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of: receiving a secure domain

Art Unit: 3992

name (Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Pages 12-13 – if the requested domain name matches a redirection rule then it is part of a domain we are proxying traffic to – the domain name is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption);

sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name (Aventail, Page 12 - “If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a False DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution,” the SOCKS server acts to resolve/request the secure computer network address from a secure domain name service);

receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name (Aventail, Page 12 – “If the destination hostname matches a redirection rule...Aventail Connect will forward the hostname to the extranet SOCKS server and the SOCKS server performs the hostname resolution.” Since the SOCKS server performs hostname resolution by requesting the secure computer network address, it is inherent that a message should be received that resolves the domain name to an address);

Art Unit: 3992

and sending an access request message to the secure computer network address using a virtual private network communication link (*Aventail, Page 77 – “The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.” – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN*).

With regards to claim 26, Aventail teaches the virtual private network includes the Internet (*Aventail, Page 5 – “Aventail...extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet”*).

With regards to claim 28, Aventail teaches the access request message contains a request for information stored at the secure computer network address (*Aventail, Page 77 – “The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.” – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN*).

With regards to claim 30, Aventail teaches the method of claim 1 performed by a software module (*Aventail, Page 7 – Aventail Connect is a client component. Aventail ExtraNet Server is a component that runs on a SOCKS 5 server; Page 9 – Aventail Connect is a layered service provider*).

Art Unit: 3992

With regards to claim 33, Aventail teaches a data processing apparatus, comprising: a processor, and memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address (*Aventail, Page 14 - Aventail Connect can be delivered on CD or as a network- delivered, self-extracting archive file; Page 15 - Aventail Connect can be installed to single workstation or to multiple networked workstations*),

said method comprising steps of: receiving a secure domain name (*Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Pages 12-13 – if the requested domain name matches a redirection rule then it is part of a domain we are proxying traffic to – the domain name is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption*);

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name (*Aventail, Page 12 - “If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a False DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution,” the SOCKS server acts to resolve/request the secure computer network address from a secure domain name service*);

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name (*Aventail, Page 12 – “If the destination hostname matches a redirection rule...Aventail Connect will forward the hostname to the extranet SOCKS server and the SOCKS server performs the hostname resolution.” Since the SOCKS server performs hostname resolution by requesting the secure computer network address, it is inherent that a message should be received that resolves the domain name to an address*);

and sending an access request message to the secure computer network address using a virtual private network communication link (*Aventail, Page 77 – “The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.” – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN*).

The rejection of claims 4, 13, 15, 20, 29, 31, and 35 as anticipated by Aventail, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as “containing the secure computer network address corresponding to the secure domain name” that is received in response to a

Art Unit: 3992

“query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Aventail fails to teach the response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above. Aventail does teach that a query message is sent to request a secure computer network address corresponding to a secure domain name (*Aventail, Page 12 –SOCKS server performs the hostname resolution*). Aventail further inherently teaches that a response message returns the secure network address because DNS resolution returns an address that corresponds to a domain name. However, Aventail does not teach that the response message includes not only the secure network address, but also VPN provisioning information.

Claims 13, 15, 29, and 31.

Claims 13 and 29 further limit their parent claims by requiring “receiving the secure domain name comprises receiving the secure domain name at a client computer from a user; wherein sending the query message comprises sending the query message at the client computer; wherein receiving the response message comprises receiving the response message at the client computer, wherein sending the access

Art Unit: 3992

request message comprises sending the access request message at the client computer." Aventail fails to teach each and every limitation and thus fails to anticipate claims 13 and 29.

Aventail teaches receiving the secure domain name comprises receiving the secure domain name at a client computer from a user (*Aventail, Page 8 – the application executes a DNS lookup. The application is run by the user at the client*);

wherein sending the query message comprises sending the query message at the client computer (*Aventail, Page 8 – the application executes a DNS lookup. The application is run on the client and thus the query message is sent at the client*);

wherein sending the access request message comprises sending the access request message at the client computer (*Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN*).

However, Aventail fails to teach receiving the response message at the client computer. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name."

Aventail fails to disclose the response message including a secure computer network address being received by the client. Instead, Aventail discloses that response messages including non-secure computer network addresses are received by the client

Art Unit: 3992

(Aventail, Page 11 – if the hostname matches a local domain string or does not match a redirection rule...performs lookup as if Aventail Connect were not running. Thus the DNS resolution response message would be returned to the client).

Aventail discloses that in the case of a request for a secure computer network address, the secure computer network address is not returned to the client (*Aventail, Page 12 – the request is for a secure computer network address when the destination hostname matches a redirection rule*). Instead, a false DNS entry is returned in a response message to the client (*Aventail, Page 12 - HOSTENT*). Thus, Aventail fails to disclose a response message being received at the client computer that includes the secure computer network address as required by claim 13.

For reasons similar to those as above, Aventail fails to anticipate claim 15 and 31's limitation requiring the method to be being performed by the client computer. As noted above, in the case of a request for a secure computer network address, Aventail fails to disclose a response message being received at the client computer that includes the secure computer network address. Thus, Aventail fails to teach "the method" being performed by the client computer.

Issue 2

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as rendered obvious by the combination of VPN Overview in view of RFC 1035 under 35 U.S.C. 103(a). These proposed rejections are adopted in part.

Art Unit: 3992

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over VPN Overview in view of RFC 1035.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 19-25 and Appendix B*).

The rejection of claims 4, 20, and 35 as unpatentable over VPN Overview in view of RFC 1035, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as “containing the secure computer network address corresponding to the secure domain name” that is received in response to a “query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Art Unit: 3992

Both VPN Overview and RFC 1035 fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above. VPN Overview teaches connection requests that result in the creation of VPN connections (*VPN Overview, Page 22 – compulsory tunneling create after initial connection is made*). In teaching VPN connections, VPN Overview's disclosures inherently teach that provisioning information is received by the client computer (*see VPN Overview, Pages 9,,26, and 27*). However, VPN Overview fails to specifically disclose the provisioning information because sent in a response message to a DNS query message.

Further, RFC 1035 fails to teach a response message containing provisioning information for the virtual private network. RFC 1035 discloses the standard for domain name resolution of Internet domain names (*RFC 1035, Page 4*). RFC 1035 discloses that in response to a user query for the resolution of a domain name; a response is received that includes the domain name address (*RFC 1035, Page 4, User responses*). However, RFC 1035's response message fails to include VPN provisioning information. Thus, Both VPN Overview and RFC 1035 fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above.

Issue 3

Art Unit: 3992

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Kosiur under 35 U.S.C. §102(b). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by Kosiur.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 25-30 and Appendix C*).

The rejection of claims 4, 20, and 35 as anticipated by Kosiur, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure

Art Unit: 3992

computer network address and (2) provisioning information for the virtual private network.

Kosiur fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to anticipate claims 4, 20, and 35. Kosiur teaches the use of DNS in order to resolve domain names into Internet addresses (*Kosiur, Page 296 – map names to addresses*). In doing so, inherently teaches that response messages are received by a client that includes the Internet address associated with a domain name (*Kosiur, Pages 293-296*). However, Kosiur fails to specifically disclose that the response message also includes provisioning information for the VPN. Kosiur never ties together the request for domain name resolution to the provisioning of the VPN. Instead, Kosiur discloses that the DNS system is split into two servers where the addresses of secure internal servers are kept separate on an isolated internal DNS server (*Kosiur, Page 296, internal DNS server*). In teaching this DNS system, Kosiur never specifically discloses that a DNS response message includes both DNS address resolution information and VPN provisioning information.

Issue 4

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Kaufman under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Art Unit: 3992

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(a)
as being anticipated by Kaufman.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33, is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 30-35 and Appendix D*).

The rejection of claims 4, 20, and 35 as anticipated by Kaufman, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as “containing the secure computer network address corresponding to the secure domain name” that is received in response to a “query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Kaufman fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to anticipate claims 4, 20, and 35. Kaufman teaches the

Art Unit: 3992

use of DNS in order to resolve the addresses of secure domain names and a response message that includes a secure computer network address (*see Kaufman, Page 127 - translate between human comprehensible addresses and IP network addresses*).

Kaufman further teaches the use of messages in order to provision a network connection to carry specified traffic from a sender to a destination (*Kaufman, Page 121 - RSVP signaling protocol*). However, Kaufman fails to teach the provisioning resulting in a response message sent back to the client that carries provisioning information. Further, Kaufman fails to tie the provisioning to DNS by failing to teach that the response message contains both DNS address resolution information and VPN information.

Issue 5

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as obvious over Kaufman in view of Galvin under 35 U.S.C. §103(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33, are rejected under 35 U.S.C. 103(a) as being obvious over Kaufman in view of Galvin.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33, is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 36-41 and Appendix E*).

The rejection of claims 4, 20, and 35 as obvious over Kaufman in view of Galvin, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as “containing the secure computer network address corresponding to the secure domain name” that is received in response to a “query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Kaufman and Galvin fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to render claims 4, 20, and 35 obvious. Kaufman teaches the use of DNS in order to resolve the addresses of secure domain names and a response message that includes a secure computer network address (see *Kaufman, Page 127 - translate between human comprehensible addresses and IP network addresses*). Kaufman further teaches the use of messages in order to provision a network connection to carry specified traffic from a sender to a destination (*Kaufman, Page 121 - RSVP signaling protocol*). However, Kaufman fails to teach the

Art Unit: 3992

provisioning resulting in a response message sent back to the client that carries provisioning information. Further, Kaufman fails to tie the provisioning to DNS by failing to teach that the response message contains both DNS address resolution information and VPN information.

On the other hand, Galvin is directed to a secure DNS system that enhances the security of the DNS system by digitally securing DNS records. Galvin also fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network. Instead, Galvin teaches a DNS response message that includes a secure computer network address, but does not include any VPN response messages (*Galvin, §3.2, resolve to user message includes IP address*).

Issue 6

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Gauntlet under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(a) as being anticipated by Gauntlet.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 40-45 and Appendix F*).

The rejection of claims 4, 20, and 35 as anticipated by Gauntlet, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as “containing the secure computer network address corresponding to the secure domain name” that is received in response to a “query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Gauntlet fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to anticipate claims 4, 20, and 35. Gauntlet inherently discloses a response message that returns a resolved computer network address by teaching the use of the DNS system to resolve computer addresses (*Gauntlet - Pages 1-8*). However, Gauntlet fails to teach the response message including any information relating to VPN provisioning. Thus, Gauntlet fails to anticipate claims 4, 20, and 35.

Issue 7

Art Unit: 3992

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as rendered obvious by the combination of Hands-On in view of Installing NT under 35 U.S.C. 103(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hands-On in view of Installing NT.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 45-52 and Appendix G*).

The rejection of claims 4, 20, and 35 as unpatentable over Hands-On in view of Installing NT, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure

Art Unit: 3992

domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Both Hands-On and Installing NT fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above. Instead, Hands-On teaches a DNUS name server that performs name resolution when it receives a DNS resolution query from a client (*Hands-On, Page 401*). In response to the DNS resolution query, the domain name is resolved to an address and is returns (*Hands-On, Page 401*). However, Hands-On does not specifically disclose that VPN provisioning information is included in that DNS response. Installing NT does not remedy Hands-On lack of teaching regarding the VPN provisioning information. Installing NT teaches the method of setting up a VPN by using Windows NT phonebook feature where the user enters the necessary VPN information including addresses, domain names, and network protocols (*Installing NT, Pages 20-23*). Installing NT does not teach the return of provisioning information to the client nor does Installing NT teach the return of provisioning information along with a DNS address resolution information in a response message.

Issue 8

Requester proposed rejections of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 as anticipated by Microsoft VPN under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(a)
as being anticipated by Microsoft VPN.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33, is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (see *Request for Reexamination, pages 52-56 and Appendix H*).

CORRESPONDENCE

All correspondence relating to this inter partes reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at <https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html>.

By Mail to: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Art Unit: 3992

For EFS-Web transmissions, 37 CFR 1.8(a)(1)(i) (C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication or earlier communications from the Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: AJK

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2009-11-25
	First Named Inventor	LARSON, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		3755-121

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

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

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

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

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

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

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

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

Application Number		
Filing Date		2009-11-25
First Named Inventor	LARSON, et al.	
Art Unit		
Examiner Name		
Attorney Docket Number		3755-121

AW	1	Exhibit 2 "Aventail Connect v3.1/v2.6 Administrator's Guide", pgs. 1-120, 1996-1999.	<input type="checkbox"/>
	2	Exhibit 3, "Windows NT Server, Virtual Private Network: An Overview", pgs. 1-28, 1998.	<input type="checkbox"/>
	3	Exhibit 4, "Network Working Group Request For Comments 1035", pgs. 1-56, 1987.	<input type="checkbox"/>
	4	Exhibit 5, "Kusiur" Building and Managing Virtual Private Networks, pgs 1-396, 1998.	<input type="checkbox"/>
	5	Exhibit 6, "Kaufman et al.," Implementing IPsec, pgs. 1-280, 1999.	<input type="checkbox"/>
	6	Exhibit 7, "James Galvin" Public Key Distribution Secure DNS, pgs. 1-12, 1996.	<input type="checkbox"/>
	7	Exhibit 8A, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs 1-137, 1998-1999.	<input type="checkbox"/>
	8	Exhibit 8B, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs. 138-275, 1998-1999.	<input type="checkbox"/>
	9	Exhibit 9, "Windows NT Technical Support: Hands On, Self Paced Training for Supporting Version 4.0", pgs. 1-106, 1998.	<input type="checkbox"/>
	10	Exhibit 10, "Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, pgs. 1-30, 1997.	<input type="checkbox"/>
	11	Exhibit 11, "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources, pgs. 1-216, 2000.	<input type="checkbox"/>

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121


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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	12/17/09
--------------------	-----------------------------------------------------------------------------------	-----------------	----------

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


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

Reexamination 	Application/Control No. 95/001,270	Applicant(s)/Patent Under Reexamination 7188180
	Certificate Date	Certificate Number

Requester Correspondence Address: <input type="checkbox"/> Patent Owner <input checked="" type="checkbox"/> Third Party
Rothwell, Figg, ^{At} Renst & Manbeck, P.C. 1425 K Street NW Suite 800 Washington, DC 20005

LITIGATION REVIEW <input checked="" type="checkbox"/>	aln <small>(examiner initials)</small>	1/7/2010 <small>(date)</small>
Case Name		Director Initials
VirnetX et'al v. Microsoft - 6:07-cv-00080-LED		<i>Eric Pearl for GM</i>

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
1.	
2.	
3.	
4.	

Search Notes 	Application/Control No. 95001270	Applicant(s)/Patent Under Reexamination 7188180
	Examiner	Art Unit 3999

SEARCHED			
Class	Subclass	Date	Examiner
709	227		

SEARCH NOTES		
Search Notes	Date	Examiner
Reviewed patented file's prosecution history	1/6/10	aln

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

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

**REEXAMINATION - PATENT OWNER
POWER OF ATTORNEY OR
REVOCATION OF POWER OF ATTORNEY
WITH A NEW POWER OF ATTORNEY
AND
CHANGE OF CORRESPONDENCE ADDRESS**

Control Number(s)	95/001,270
Filing Date(s)	12/08/09
First Named Inventor	Victor Larson
Title	Method for Establishing Secure...
Patent Number	7,188,180
Examiner Name	Lim, Krisna
Attorney Docket No(s).	77580-0090

I hereby revoke all previous patent owner powers of attorney given in the above-identified reexamination proceeding control number(s).

A Power of Attorney is submitted herewith.

OR

I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

23630

OR

I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified reexamination proceeding control number(s) (more than one may be changed only if they are merged proceedings) to be:

The address associated with the above-mentioned Customer Number.

OR

The address associated with Customer Number:

OR

Firm or Individual Name

Address

City State Zip

Country

Telephone Email

I am the:

Inventor, having ownership of the patent being reexamined.

OR

Patent owner.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Inventor or Patent Owner

Signature	<i>Victor J. Larson</i>	Date	1/2/2010
Name	Victor J. Larson	Telephone	703-359-4649
Title and Company	R+D Director VirnetX		

NOTE: Signatures of all the inventors or patent owners of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

*Total of 1 forms are submitted.

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

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

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

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: VirnetX Inc.

Application No./Patent No.: 7,188,180 Filed/Issue Date: 03/06/2007

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

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

states that it is:

- 1. the assignee of the entire right, title, and interest in;
- 2. an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or
- 3. the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

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

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

OR

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

1. From: Larson et al. To: Science Applications International Corp.

The document was recorded in the United States Patent and Trademark Office at Reel 014679, Frame 0947, or for which a copy thereof is attached.

2. From: Science Applications International Corp. To: VirnetX Inc.

The document was recorded in the United States Patent and Trademark Office at Reel 018757, Frame 0326, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

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

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 902.08]

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

[Signature]
Signature
Randall Larson
Printed or Typed Name

12/15/09
Date
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-8199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	6855360
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	3755-121
Receipt Date:	21-JAN-2010
Filing Date:	08-DEC-2009
Time Stamp:	15:40:56
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	ReexamPOA.pdf	67354 <small>978fe33d73fbad051007559e599897ecff68870</small>	no	1

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2	Assignee showing of ownership per 37 CFR 3.73(b).	Larson_Statement.pdf	743249 d7d8549a8d0fd27801e95429654a26a3cf6497fd	no	1
---	---------------------------------------------------	----------------------	----------------------------------------------------	----	---

Warnings:

Information:

Total Files Size (in bytes):	810603
-------------------------------------	--------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

REEXAMINATION - PATENT OWNER POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS	Control Number(s)	95/001,270
	Filing Date(s)	12/08/09
	First Named Inventor	Victor Larson
	Title	Method for Establishing Secure...
	Patent Number	7,188,180
	Examiner Name	Lim, Krisna
	Attorney Docket No(s).	77580-0090

I hereby revoke all previous patent owner powers of attorney given in the above-identified reexamination proceeding control number(s).

A Power of Attorney is submitted herewith.

OR

I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 23630

OR

I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified reexamination proceeding control number(s) (more than one may be changed only if they are merged proceedings) to be:

The address associated with the above-mentioned Customer Number.

OR

The address associated with Customer Number:

<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

I am the:

Inventor, having ownership of the patent being reexamined.

OR

Patent owner.
 Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Inventor or Patent Owner

Signature	<i>Victor J. Larson</i>	Date	1/2/2010
Name	Victor J. Larson	Telephone	703-359-4649
Title and Company	R&D Director Vlnetix		

NOTE: Signatures of all the inventors or patent owners of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below

Total of 1 forms are submitted.

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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



Bib Data Sheet

CONFIRMATION NO. 2128

SERIAL NUMBER 95/001,270	FILING OR 371(c) DATE 12/08/2009 RULE	CLASS 709	GROUP ART UNIT 3992	ATTORNEY DOCKET NO. 3755-121
------------------------------------	-----------------------------------------------------------	---------------------	-------------------------------	----------------------------------------

APPLICANTS
 7188180, Residence Not Provided;
 VIRNETX INC.(OWNER), SCOTTSVALLEY DRIVE, CA;
 MICROSOFT CORPORATION(3RD. PTY. REQ.), CHEVY CHASE, MD;
 MICROSOFT CORPORATION(REAL PTY. IN INTEREST), CHEVY CHASE, MD;
 ROTHWELL, FIGG, ERNST & MANBECK, P.C., WASHINGTON, DC

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

**** FOREIGN APPLICATIONS *******

Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after Allowance				
Verified and Acknowledged	Examiner's Signature	Initials		

ADDRESS
 23630

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

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	<input type="checkbox"/> All Fees
		<input type="checkbox"/> 1.16 Fees (Filing)
		<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)
		<input type="checkbox"/> 1.18 Fees (Issue)
		<input type="checkbox"/> Other _____
		<input type="checkbox"/> Credit



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,270	12/08/2009	7188180	3755-121

CONFIRMATION NO. 2128

POA ACCEPTANCE LETTER

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



Date Mailed: 01/22/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/14/2010.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/sdstevenson/

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,270	12/08/2009	7188180	3755-121

CONFIRMATION NO. 2128

POWER OF ATTORNEY NOTICE



22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Date Mailed: 01/22/2010

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/14/2010.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/sdstevenson/

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
Edmund Munger, et al.)
)
U.S. Patent No.: 7,188,180)
Filed: November 7, 2003) Examiner:
Issued: March 6, 2007) Andrew L. Nalven
)
For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
SECURE COMMUNICATION LINK)
BETWEEN COMPUTERS OF)
VIRTUAL PRIVATE NETWORK)
)
Reexamination Proceeding)
Control No.: 95/001,270)
Filed: December 8, 2009)

**PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.956 TO REPLY TO
OFFICE ACTION IN REEXAMINATION**

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. § 1.956, the Patent Owner respectfully requests a two-month extension of time to respond to the Office Action mailed January 19, 2010 (“the Office Action”). The current deadline for response is March 19, 2010. A two-month extension would extend the deadline to May 19, 2010.

For reasons stated more fully below, the extension of time requested is necessary to fully and completely address the §§ 102 and 103 rejections in the Office Action. The complexity of

the issues raised by the Office Action is exacerbated by (1) the need to investigate the inventive activities behind any and/or all of the rejected claims and the corresponding possibility that at least the Aventail Connect Administrator's Guide ("Aventail"), upon which a § 102(a) rejection is based, is not proper prior art, and (2) the consideration of whether a § 1.132 declaration from a technical expert is appropriate and, importantly, is available under the constraints imposed by the current period for response. Further straining the ability of the Patent Owner to respond to the outstanding rejections are (1) the delay in the Patent Owner's receiving the Office Action after it was mailed, (2) a concurrent trial involving the above-referenced patent, which has caused a significant drain on the Patent Owner's resources, especially the inventors who are necessary to prepare a proper response to the Office Action, and (3) the concurrent reexamination proceedings of a patent related to the above-referenced patent, described below, which has also caused a significant drain on the availability of the Patent Owner's resources. In light of these factors, as more fully explained below, the Patent Owner respectfully requests a two-month extension of time to May 19, 2010 to respond to the outstanding Office Action.

I. Delay in Receipt of The Office Action

Preliminarily, the Patent Owner lost several important and useful days of the period for response. Despite having a mailing date of January 19, 2010, the Office Action was not received by the Patent Owner until January 26, 2010. The Patent Owner filed a Power of Attorney for U.S. Patent No. 7,188,180 ("the '180 patent") on December 15, 2009, which was accepted on December 30, 2009. Because the Patent Owner had not received a Notice of Acceptance, it filed another Power of Attorney on January 14, 2010, before the mailing of the Office Action. This second Power of Attorney was not accepted until January 22, 2010. Despite the Patent Owner's efforts, the Office Action was mailed to its prior patent counsel, who then forwarded the Office Action to the Patent Owner's current counsel on January 25, 2010. For this reason, the Patent Owner did not receive the Office Action until after a critical week of its time period for response expired.

II. Complexity of The Office Action

Preparing a response to the Office Action will involve substantial analysis requiring significant time and resources. Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 patent are

rejected under 35 U.S.C. §§ 102 and 103 as allegedly being anticipated by and/or rendered obvious by combinations of Aventail, the *VPN: An Overview* reference, the *Network Working Group RFC: 1035* reference, the *Building and Managing Virtual Private Networks* reference by Kosiuer, the *Implementing IPsec* reference by Kaufman, the *Public Key Distribution with Secure DNS* reference by Galvin, the *Gauntlet Firewall for Windows NT Administrator's Guide* reference, the *Windows NT Technical Support: Hands-On* reference, the *Installing, Configuring, and Using PPTP* white paper, and the *Building a Microsoft VPN* reference (collectively “the References”). Preparation of a response to the outstanding Office Action (“the Response”) naturally requires substantive analysis of the References and comparison of them to the thirteen rejected claims. The References describe complex systems spanning over 1500 pages. While the Patent Owner has reviewed the References in its due diligence conducted to date, the complexity of each of the References requires a more in depth analysis and comparison by personnel of the Patent Owner, including one or more of the inventors, whose availability within the two month period for response to the Office Action has been and will continue to be limited, as discussed below.

In addition, due to the considerable ramifications of canceling or amending the rejected claims, the Patent Owner believes it necessary to consider providing the Examiner with the views of an independent technical expert in a § 1.132 declaration. To date, the Patent Owner has actively considered the use of and investigated several candidates to serve as a technical expert for providing such a § 1.132 declaration. It has proven extremely difficult to locate such an expert who can provide fully informed views within such a short time-frame – several contacted so far have expressed that there is insufficient time to tackle all of the relevant issues in the time permitted by the current deadline for a response to the Office Action.

The Patent Owner also is necessarily investigating the relevant dates of conception and reduction to practice, as well as diligence therebetween, of the inventions defined in one or more of the rejected claims to determine which of those activities predates the date of publication of one or more of the References, including, for example, Aventail, and, thus, whether or not one or more of the References, including Aventail, constitutes prior art to one or more of the rejected claims. This investigation necessarily requires significant time from the Patent Owner during a time when its relevant personnel, including one or more of the inventors, are strained for time

and attention as a result of their other duties in the co-pending reexamination and the concurrent litigation.

II. Concurrent Litigation and Trial Proceedings

Just at the time when the Patent Owner is in need of significant resources to respond to the Office Action, many of those very resources are now heavily taxed by the pending litigation proceedings involving the '180 patent and others. As mentioned in the Replacement Request for *Inter Partes* Reexamination of Patent, the '180 patent is currently a subject of litigation in Case No. 6:07-cv-80 in the Eastern District of Texas captioned *VirnetX, Inc. v. Microsoft Corp.*, a litigation in which the Requester itself is involved. As provided in the Court's Scheduling Order of June 30, 2009, the jury trial in this litigation is scheduled to begin on March 8, 2010 (following jury selection on March 1, 2010), a mere eleven days before the response to the Office Action is currently due. Various personnel of the Patent Owner are spending significant time in preparing for that trial. As a result, resources and personnel of the Patent Owner required to fully and accurately prepare a response to the Office Action are temporarily limited while the time-consuming trial preparations are conducted as the trial in Texas nears.

While the Patent Owner's counsel continues to perform its due diligence for responding to the Office Action, the looming trial proceedings will make it difficult to complete the Patent Owner's diligence by the current March 19 deadline for response to the Office Action. Moreover, not only would a two month extension permit the resources to be dedicated to responding to this Office Action, it would likely also permit consideration of any court conclusions regarding the claims presently under reexamination.

III. Concurrent Reexamination of Patent No. 6,502,135

Further straining the circumstances are the concurrent *inter partes* reexamination proceedings involving related Patent No. 6,502,135 ("the '135 patent"), which is also at issue in the above-mentioned litigation and is also initiated by the Requester who is involved in litigation. The Office Action mailed January 15, 2010 in the re-examination of the '135 patent ("the Related Reexamination") requires a response due March 15, 2010 – four days before the due date for the response to the Office Action in the present case (a petition for an extension of time is similarly being filed in the Related Reexamination.).

Analyzing the Office Action in preparation for a response in the Related Reexamination has already taken a significant amount of the Patent Owner's resources and personnel, including one or more of the inventors, and will require more of their time in the future. Accordingly, responding to the present Office Action has taken, continues to take, and will continue to take a large amount of the very personnel and resources that are necessary at trial and in the Related Reexamination.

IV. Conclusion

For the reasons stated above, the Patent Owner believes that a two-month extension is appropriate. A prompt decision granting this extension of time is respectfully requested to allow the Patent Owner a fair opportunity to respond to the present Office Action.

Please charge any shortage in fees due in connection with the filing of this paper, including the petition fee of \$200.00 set forth in 37 C.F.R. § 1.17(g), to Deposit Account 501133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/

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

Matthew E. Leno, Reg. No. 41,149

Hasan M. Rashid, Reg. No. 62,390

McDermott Will & Emery LLP

Attorneys for Applicant

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com
mleno@mwe.com
hrashid@mwe.com
Date: February 22, 2010

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

Electronic Patent Application Fee Transmittal

Application Number:	95001270
Filing Date:	08-Dec-2009
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	077580-0090

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Petition fee- 37 CFR 1.17(g) (Group II)	1463	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				200

Electronic Acknowledgement Receipt

EFS ID:	7061278
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	22-FEB-2010
Filing Date:	08-DEC-2009
Time Stamp:	17:40:23
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$200
RAM confirmation Number	4319
Deposit Account	501133
Authorized User	

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

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

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Request for Extension of Time	Petition_Extension_180.pdf	126231 9cc5b00ff77e16dd51a62a1b3c55f1d0b394d d0bf	no	5
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30504 991e8d9e9d9584340ec76053ad061c49c20 6453d	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			156735		
<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

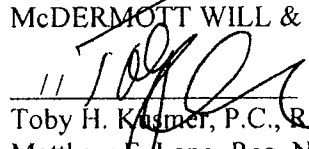
In the Reexamination of:)	
Edmand Munger, et al.)	
)	
U.S. Patent No.: 7,188,180)	
Filed: November 7, 2003)	Examiner:
Issued: March 6, 2007)	Andrew L. Nalven
)	
For: METHOD FOR ESTABLISHING)	Group Art Unit: 3992
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF VIRTUAL)	
PRIVATE NETWORK)	
)	
Reexamination Proceeding)	
Control No.: 95/001,270)	
Filed: December 8, 2009)	

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Petition for Extension of Time Under 37 C.F.R. § 1.956 to Reply to Office Action in Reexamination, filed with United States Patent and Trademark Office on February 22, 2010, was served this 22nd day of February, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP


 // Toby H. Kusmer, P.C., Reg. No. 26,418
 Matthew E. Leno, Reg. No. 41,149
 Hasan M. Rashid, Reg. No. 62,390
 McDermott Will & Emery LLP
 Attorneys for Applicant

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

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: February 22, 2010

Electronic Acknowledgement Receipt

EFS ID:	7062751
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Michael A. Messina/4252/Matilda Mason
Filer Authorized By:	Michael A. Messina
Attorney Docket Number:	077580-0090
Receipt Date:	22-FEB-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:59:44
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Certificate of Service	077580-0090Certificate.pdf	33031 e3dd6691fd2d72218676cb546b62b334de e9b6b	no	1

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re-Exam
Application
Control No. 95/001,270

RECEIVED

Confirmation No. 2128

FEB 23 2010

Based on U.S.
Patent No. 7,188,180
First Named
Inventor Victor Larson

CENTRAL REEXAMINATION UNIT

Issued: 06/06/2007

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

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 2/23/10.

Examiner: Andrew L. Nalven


Atabak Royace

Art Unit 3992

Mail Stop: Inter Partes Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

- 1) Information Disclosure Statement (2 pages)
- 2) Information Disclosure Statement by Applicant (Form 1449) (19 pages);
- 3) Copies of references listed in the IDS Form 1449 as follows:


References	Express Mail Tracking No
Box 1 containing references B1000-B1002 & C998-C1060;	EV643770648US
Box 2 containing references C1061-C1080;	EV643770951US
Box 3 containing references C1081-C1105;	EV643770665US
Box 4 containing references C1106-C1152;	EV643770679US
Box 5 containing references C1153-C1205;	EV643770682US
Box 6 containing references C1206-C1212; and	EV643770696US
Box 7 containing references C 1213-C1242	EV643770705US

- 4) Return receipt postcard.

There are no fees due with the filing of this Information Disclosure Statement. However, the Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

McDermott, Will & Emery LLP



Toby H. Kusmer, Reg. No. 26,418

Atabak R. Royae, Reg. No. 59,037

McDermott Will & Emery LLP

28 State Street

Boston, MA 02109-1775

Telephone: (617) 535-4065

Facsimile: (617) 535-3800

Date: February 23, 2010

Docket No.: 077580-0090

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re-Exam
Application
Control No. 95/001,270

Confirmation No. 2128

Based on U.S.
Patent No. 7,188,180
First Named
Inventor Victor Larson

Issued: 06/06/2007

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

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 2/23/07.

Examiner: Andrew L. Nalven


Atabak Royace

Art Unit 3992

Mail Stop: Inter Partes Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97, 1.98 and 1.555, 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 reexamination of the above-referenced patent, and that the documents be made of record therein and appear among the "References Cited" on any Re-examined patent to issue therefrom.

Documents A1000-A1039, B1000-B1002 and C998-C1241 listed in the enclosed form PTO-1449 have been produced by Microsoft Corp. in VirnetX Inc. and Science Applications International Corp. v. Microsoft Corp. civil action currently pending before the U.S. District Court for the Eastern District of Texas.

Document C1242 is an Inter Partes Reexamination Request filed for U.S. Patent No. 6,502,135, which is related to the above-referenced patent and is concurrently undergoing reexamination proceedings.

Although the undersigned attorney has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. Enclosed are 7 boxes containing foreign patent documents B1000-B1002 and non-patent literature documents C998-C1242 as indicated in form 1449 enclosed herewith. The Examiner is invited to call the undersigned attorney for any questions regarding any of these documents.


This Statement is not to be interpreted as a representation that the cited publications are material, 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.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

The commissioner is hereby authorized to charge any fees required 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



Toby H. Kusmer, Reg. No. 26,418

Atabak R. Royae, Reg. No. 59,037

28 State Street

Boston, MA 02109

Phone: 617-535-4065

Facsimile: 617-535-3800

Date: 2/23/2010

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

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 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	5,303,302	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
----------	-----------------

*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	2	of	19		

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
	A1033	6,314,463	11/06/01	Abbott, et al.	
	A1034	6,298,341	10/02/01	Mann, et al.	
	A1035	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1036	6,199,112	03/06/04	Wilson, Stephen K.	
	A1037	6,052,788	04/18/00	Wesinger, et al	
	A1038	2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1039	2001/0049741	12/06/01	Skene, et al.	
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	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
	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				DATE CONSIDERED			

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, FreeS/WAN)			
	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, FreeS/WAN)			
	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, FreeS/WAN)			
	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.			
	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/soc kswp.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		

*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, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)			
	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.			
	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 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)			
	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)			
	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		

*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.			
	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	

*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.			
	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 <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	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.			
	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	Publicly available emails relating to FreeSWAN (MSFTVX00018833-MSFTVX00019206). (FreeSWAN emails, FreeSWAN)			
	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	

*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.			
	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.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)			
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	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.			
	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)			
	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 Winlnet</i> 313-423 (Addison Wesley Longman 1998) (Essential Winlnet)			
	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)			
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	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.			
	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.mspix (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)			
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), <i>available at</i> http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspix (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, <i>available at</i> http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspix (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, <i>Available at</i> http://www.microsoft.com/technet/archive/winntas/proddocs/ras40/rasch01.mspix (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, <i>available at</i> http://www.microsoft.com/technet/archive/winntas/proddocs/ras40/rasch05.mspix (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		

*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.			
	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)			
	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		

*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.			
	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 Thing 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 FreeS/WAN Overview (1999) (Linux FreeS/WAN) 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		

*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.
	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
----------	-----------------

*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.			
	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	

*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	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, VirmetX 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 <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	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.			
	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			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 1643905-1.077580.0090



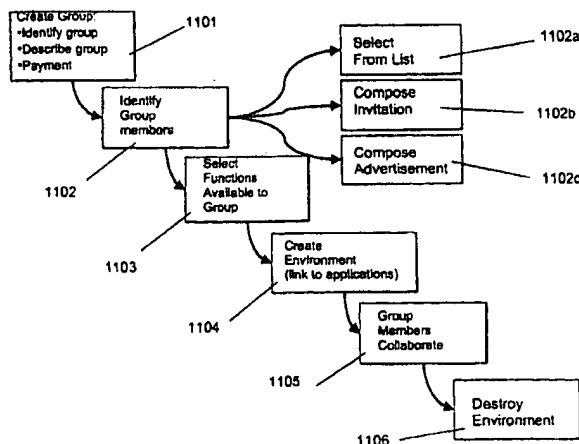
PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁷ : G06F 17/00</p>	<p>A2</p>	<p>(11) International Publication Number: WO 00/17775 (43) International Publication Date: 30 March 2000 (30.03.00)</p>
<p>(21) International Application Number: PCT/US99/21934 (22) International Filing Date: 22 September 1999 (22.09.99) (30) Priority Data: 60/101,431 22 September 1998 (22.09.98) US 09/399,753 21 September 1999 (21.09.99) US (71) Applicant (for all designated States except US): SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): MILLER, Craig [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). MANGIS, Jeffrey, K. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). LESTER, Harold, D. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). NICHOLAS, John, M. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). WALLO, Andrew [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US).</p>		<p>(US). KRESS, Thomas, P. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). CHEAL, Linda, J. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). WEATHERBEE, James, E., Jr. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). DAVIES, Linda, M. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). (74) Agents: WRIGHT, Bradley et al.; Banner & Witcoff, Ltd., Eleventh floor, 1001 G Street, N.W., Washington, DC 20001-4597 (US). (81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>Without international search report and to be republished upon receipt of that report.</i></p>

(54) Title: USER-DEFINED DYNAMIC COLLABORATIVE ENVIRONMENTS



(57) Abstract

A collaborative system and method allows members of a group to collaborate on a project such as a bid or proposal. According to a first embodiment, a complex instrument trading engine (CITE) facilitates negotiation between two or more parties. A set of tools and techniques are provided in order to facilitate negotiation and execution of complex instruments such as contracts between corporations and governments. According to a second embodiment, referred to as a dynamic collaborative environment, a user can define a group and a virtual private network environment including user-selected tools that facilitate communication, research, analysis, and electronic transactions within the group. The environment can be destroyed easily when it is no longer needed. Multiple environments can co-exist on the same physical network of computers.

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	Licchtenstein	SD	Sudan		
DE	Gennany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

1 **USER-DEFINED DYNAMIC COLLABORATIVE ENVIRONMENTS**

2 This application is related in subject matter to and claims priority from
3 provisional U.S. application serial number 60/101,431, filed on September 22, 1998.

4 The contents of that application are bodily incorporated herein.

5 **BACKGROUND OF THE INVENTION**

6 1. Technical Field

7 This invention relates generally to computer systems and networks. More
8 particularly, the invention relates to systems and methods for providing user-defined
9 collaborative environments for transacting business or electronic commerce.

10 2. Related Information

11 Following hurricane Andrew, many insurance companies sought to limit their
12 risk by withdrawing coverage from coastal areas. While this made good sense for the
13 specific companies, it was not acceptable from a societal perspective. The cities,
14 towns, homes and businesses built near the coasts could not afford to go without
15 insurance, nor could the financial institutions that loaned money on these properties
16 afford the risk. The problem facing the insurance companies was not the absolute
17 magnitude of the risk, but the concentration of the risks in one area, leading to the
18 possibility of very large losses resulting from a single event.

19 One law firm had conceived the idea of providing a mechanism for insurance
20 companies to exchange risk. Companies with a high exposure in one area (e.g.
21 Florida windstorms) could reduce their risk by ceding part of this to another company
22 with non-coincident risk (e.g. California earthquakes) and assume part of the second
23 company's risk in return. A company (CATEX) was formed to conduct such trading,
24 but the trading rules had yet to be defined and the trading infrastructure had not yet
25 been developed. CATEX postulated that the key barrier to insurance risk trading was
26 determining the relative risk of different perils in different regions. One approach
27 suggested by CATEX was to try to estimate these relative risks (termed relativities)
28 for a broad set of perils and regions, to provide an initial basis for trading.

29 It was recognized, for various reasons, that this could not be done feasibly
30 because: general estimates of risk, rather than the risk for specific locations,
31 buildings, ships, etc. would be inadequate for commerce; there were many risks to
32 evaluate given all of the permutations of location, perils, and structure; and
33 companies would not be willing to trade risk based strictly on a third-party's analysis

1 An analysis of the problem, however, indicated that estimating the relativities
2 was not essential to facilitate trading, or, in a broader sense, that trading was the only
3 way to address the problem of insuring concentrated risk. The key difficulty was
4 determining how to create greater efficiency in the reinsurance market, whether by
5 introducing new instruments (like swaps), bringing new capital to the market,
6 connecting more buyers to more traders, or reducing the cost of placing reinsurance.
7 It was determined that the above concept could be implemented in an electronic
8 trading system that could play an important role in promoting these factors, and
9 could, in fact, transform the reinsurance market, which is not very automated. A
10 system that allowed trading was developed and implemented. A more detailed
11 description of this system, as enhanced in accordance with various inventive
12 principles herein (referred to as "first-generation" complex instrument trading
13 technology), are provided below. More generally, as electronic commerce (and
14 business-to-business commerce, in particular) has grown, various companies have
15 developed software tools and services to facilitate transactions on the Internet and
16 over private networks. E-Bay, for example, hosts a well-known web site that
17 operates a transaction model (a so-called "concurrent auction") that permits buyers
18 to submit bids on items offered by individuals. Lotus Notes provides a network-
19 oriented system that allows users within a company to collaborate on projects.
20 Oracle Corporation hosts various transaction engines for clients that pay to host such
21 services on a web site. DIGEX Corporation similarly hosts web-based application
22 programs including various transaction engines. Other companies sell so-called
23 "shrink wrap" software that allows individuals to set up web sites that provide
24 catalog ordering facilities and the like.

25 Some Internet service providers, such as America Online, host "chat rooms"
26 that permit members to hold private discussions with other members who enter
27 various rooms associated with predetermined topics. A company known as
28 blueonline.com hosts a web site that facilitates collaboration on construction projects.
29 Various virtual private networks have been created to facilitate communication
30 among computer users across the Internet and other networks, but these networks
31 provided very limited functionality (e.g., e-mail services); are not user-defined (they
32 must be created and installed by system administrators); and they cannot be easily
33 destroyed when they are no longer needed.

1 The aforementioned products and services are generally not well suited to
2 facilitating complex electronic transactions. As one example, most conventional
3 services are predefined (not user-defined) and are centrally administered. Thus, for
4 example, a group of companies desiring to collaborate on a project must fit their
5 collaboration into one of the environment models provided by an existing service
6 provider (or, alternatively, build a custom system at great expense).

7 Suppose, for example, that a group of high school students needs to
8 collaborate on a research paper that requires soliciting volunteers for a survey on drug
9 use, conducting the survey, brainstorming on the survey results, posing follow-up
10 questions to survey participants anonymously, publishing a report summarizing the
11 results, and advertising the report for sale to newspapers and radio stations. This
12 project requires elements of communication among persons inside a defined group
13 (those writing the paper) and outside the group (e.g., survey participants); conducting
14 research (conducting the survey, compiling the results, comparing the results with
15 other surveys published by news sources; and brainstorming on the meaning of the
16 results); and conducting a commercial transaction (e.g., publishing the survey in
17 electronic form and making it available at a price to those who might be interested
18 in the results). No existing software product or service is available to meet the
19 specific needs of this research team. Creating a user-defined environment including
20 tools and communication facilities to perform such a task would be prohibitively
21 expensive. Even if such a tailor-made environment could be created, it would be
22 difficult to disassemble the environment (computers, networks, and software) after
23 the project was completed.

24 In short, there is a need to provide a user-defined collaborative environment
25 that is tailored to the needs of particular groups that conduct communication,
26 research, electronic transactions, and deal-making.

27 **SUMMARY OF THE INVENTION**

28 A first embodiment of the invention, referred to as a complex instrument
29 trading engine (CITE), facilitates negotiation between two or more parties. In this
30 embodiment, a set of negotiation tools and techniques such as anonymous email,
31 secure communication, document retention, and bid and proposal listing services are
32 provided in order to facilitate the negotiation and execution of complex instruments
33 such as contracts between corporations, governments, and individuals.

1 A second embodiment of the invention, referred to as a dynamic collaborative
2 environment (DCE), allows members of a group to define a dynamic virtual private
3 network (DVPN) environment including user-selected tools that facilitate
4 communication, research, analysis, and electronic transactions both within the group
5 and outside the group. The environment can be destroyed easily when it is no longer
6 needed. Multiple environments can co-exist on the same physical network of
7 computers.

8 Although the two embodiments are described separately for ease of
9 comprehension, it should be understood that the two embodiments share many
10 features and, in fact, the second embodiment could include some or all of the features
11 of the first embodiment in a generalized collaborative system. Consequently,
12 references to a specific embodiment in the following description should not be
13 deemed to limit the scope of features or tools included in each embodiment.
14 Moreover, references to specific applications, such as the reinsurance industry,
15 should not be deemed to limit the application of the invention to any particular field.

16 **BRIEF DESCRIPTION OF THE DRAWINGS**

17 FIG. 1A shows a four-step model of deal making including meeting, analysis,
18 negotiation, and closing the deal.

19 FIG. 1B shows contract formation among a group of parties to a contract.

20 FIG. 2 shows a listing display system showing all offers for contracts and
21 responses thereto.

22 FIG. 3 shows details of a listing that has been selected by a user.

23 FIG. 4 shows one possible implementation of a reply card definition screen.

24 FIG. 5 shows one possible implementation of a document management
25 screen.

26 FIG. 6 shows one possible implementation of a screen indicating persons
27 having access to a shared folder.

28 FIG. 7 shows a list of consummated deals in the system.

29 FIG. 8A shows detailed information regarding a completed trade.

30 FIG. 8B shows a deal summary including structured and unstructured
31 information concerning the deal.

32 FIG. 9 shows a "flip widget" in a first state.

33 FIG. 10 shows a "flip widget" in a second state.

1 FIG. 9A shows a more detailed example of a "flip widget" in a first state.
2 FIG. 10A shows a more detailed example of a "flip widget" in a second state.
3 FIG. 11 shows method steps that can be carried out to define, create, and
4 destroy an environment according to a second embodiment of the invention.
5 FIG. 12 shows one possible system architecture in which various principles
6 of the invention can be implemented.
7 FIGS. 13A through 13C show one possible user interface for creating a group
8 and identifying group members.
9 FIG. 14A shows one possible user interface for selecting group members from
10 one or more lists.
11 FIG. 14B shows one possible user interface for selecting group members by
12 composing invitations.
13 FIG. 14C shows one possible user interface for selecting group members by
14 composing an advertisement.
15 FIG. 15 shows a banner advertisement 1501 displayed on a web site, wherein
16 the banner advertisement solicits participation in a group.
17 FIG. 16 shows one possible user interface for selecting communication tools
18 to be made available to group members.
19 FIG. 17 shows one possible user interface for selecting research tools to be
20 made available to group members.
21 FIG. 18 shows one possible user interface for selecting transaction engines
22 to be made available to group members.
23 FIG. 19 shows one possible user interface for selecting participation engines
24 to be made available to group members.
25 FIG. 20A shows an authentication screen for group members to gain access
26 to a newly created environment.
27 FIG. 20B shows a web page generated for a specific user-defined
28 environment, including tools available to group members having access to the
29 environment.
30 FIG. 21 shows one possible method of generating environments in accordance
31 with various aspects of the present invention.
32 FIG. 22 shows one possible data storage arrangement for storing and
33 manipulating brain writing cards.

1 **DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

2 **A. COMPLEX INSTRUMENT TRADING ENGINE EMBODIMENT**

3 A first embodiment of the present invention provides a second-generation
4 version of a complex instrument trading system. The second-generation system
5 includes specialized tools that were not included in the first version of the prior art
6 CATEX insurance trading system described above. These tools represent a
7 substantial improvement over the first generation and incorporate new concepts of
8 communications in a trading environment, and other capabilities that did not exist in
9 the first generation technology. In addition, it is believed that many of these tools are
10 also applicable to software systems other than the Complex Instrument Trading
11 Engine or Negotiating System (CITE) described herein. Thus, the inventive
12 principles are not limited to trading systems for complex instruments, nor even to
13 trading systems in general.

14 Primarily, the tools described herein ameliorate certain difficulties associated
15 with trading of complex instruments. Complex instruments are instruments where
16 there is more than one dimension for negotiation. As compared to such instruments
17 as securities, complex instrument transactions take longer to research and
18 consummate and require more extensive documentation. For example, stock trading
19 employs a simple instrument (a share) and negotiation focuses on one dimension
20 (price) while insurance contracts have many dimensions (term, price, coverage,
21 definitions of perils, etc.). The stock market is relatively simple to automate -- as
22 soon as bid and asked prices match, the deal is concluded in an instant according to
23 the rules of the exchange. Automation of complex trading is much more difficult,
24 since the parties must negotiate and reach agreement on multiple dimensions and
25 document that agreement using an instrument specific to the precise agreement.
26 Automation of complex instrument trading is more difficult in every way than trading
27 simple instruments.

28 The trading model behind the Complex Instrument Trading Engine or
29 Negotiating System is built around a simple, four-step model of deal making.
30 Referring to FIG. 1A, the steps are as follows:

31 1. Meeting: Potential buyers connect with potential sellers with reciprocal
32 interests. This connection does not mean that a deal will necessarily be concluded but
33 simply that the two parties have some basis for continuing discussion. In simple

1 instrument trading, it is typically only necessary to advertise quantity and price
2 offered or sought. Offers for complex instruments must include substantially more
3 detail and (frequently) extensive attachments or exhibits.

4 2. Research/Analysis: Each company considers its own position and/or offer
5 and the counter party's position. Using information and analytic tools from various
6 sources, including internal resources and resources provided by or through the trading
7 system, each party does research and refines its position. The multiple dimensions
8 of complex instruments increases the analytical complexity and limits the value of
9 a simple market price. As indicated by the arrows in FIG. 1, this step is usually
10 performed iteratively with the negotiation.

11 3. Negotiation: Parties to the negotiation speak directly and exchange
12 whatever information is necessary to advance the deal. As indicated by the arrows
13 in FIG. 1A, this step is usually performed iteratively with the research step.

14 4. Close: the companies negotiate and sign an instrument that documents the
15 deal. This can be a complete and detailed contract, or it may be a simple
16 memorandum. In simple instrument trading, the actual trade agreement is often
17 standardized by the exchange. In complex instrument trading, the agreement must
18 be more specific to the deal, though it is possible to use such tools and fill-in-the
19 blank forms.

20 Within a system using these complex instrument tools, trading parties can
21 place offers to buy, sell, or trade in a public area, and examine such offers ("listings")
22 posted by others. Using advanced communications tools the parties can conduct
23 initial discussions to determine if a placement is possible. Using tools described
24 herein, the initial contact can be done anonymously.

25 If a deal seems possible, the system preferably provides access to the
26 extensive information necessary to assess the possible deal. This can include static
27 information (e.g. reports or data) maintained within the system, links to information
28 providers outside the system, online analytical tools, and links to providers of
29 analytical services.

30 For complex instruments, the process of negotiating a deal is contemplated
31 to be an iterative one, with successive stages of analysis and discussion. The need
32 for extensive communication is one of the critical distinctions between trading of
33 simple instruments (e.g. retail sale) and complex instruments. Complex instrument

1 trading requires dialog and more -- exchange of documents (often voluminous),
 2 consultation with counsel and intermediaries, conferencing, and working together on
 3 the final agreement. For electronic commerce to have an impact in complex
 4 instrument trading, it must support and facilitate this communication, and not force
 5 traders to fall back on methods and technology outside the electronic trading
 6 environment.

7 The final step is closing the deal. The companies can negotiate a contract
 8 online. Tools provide sample, fill-in the blank contracts and memoranda of
 9 understanding as a starting point. Negotiators can begin with these, or they can use
 10 one of their own. Collaborative software makes it possible to display text
 11 simultaneously on each negotiator's screen and to work on the language together.
 12 When the contract is final, the system allows for secure, online signature, though
 13 companies not comfortable with electronic signature for very large deals may print
 14 a hard copy and sign it conventionally.

15 By creating electronic exchanges for complex instrument trading, the CITE
 16 tools can have a fundamental and positive impact on many areas of commerce:

17 1. An electronic exchange makes it possible to put an offer in front of more
 18 people more quickly than could be informed through direct contact, even allowing
 19 for active intermediaries or brokers.

20 2. Traders can advertise and conclude deals without the need for an
 21 intermediary when they have adequate support or internal resources.

22 3. Through better communications, wider exposure for offers, and the first
 23 steps towards standard contract language, electronic trading of complex instruments
 24 can substantially reduces transaction costs.

25 4. With lower transaction costs, it is possible to conclude deals that were not
 26 possible with higher overhead.

27 5. Through the immediate posting of the results of trades, pricing is moved
 28 towards a market basis, reducing research and analysis costs enormously. This
 29 speeds placement.

30 6. Smaller exposure means lower risk, and market pricing is an adequate
 31 surrogate for analytically derived pricing in some circumstances. Together these
 32 factors make it possible for traders to participate in markets or market segments in
 33 which they would not normally do business.

1 7. By making it possible for all companies, large and small, to talk directly
 2 to each other, electronic trading of complex instruments can lead to the
 3 democratization of the marketplace increasing competition.

4 Overall, electronic trading of complex instruments has the potential to
 5 improve the efficiency of markets enormously, and to establish markets in areas of
 6 commerce that are currently done through intermediaries or on a one-on-one basis.

7 The trading tools described herein are designed to facilitate electronic trading of
 8 complex instruments. The first-generation complex instrument trading tools broke
 9 new ground in the extension of electronic commerce into new and more complicated
 10 markets. The table below summarizes the areas of new and improved technology,
 11 organized into the four steps of the general complex instrument trading model.

Phase	First Generation Complex Instrument Trading Technology (PRIOR ART)	Advanced Complex Instrument Trading Technology
Meet	<ul style="list-style-type: none"> • Operates on private network only • Post a listing to board by filling out a form • Display listing summary in a table • Search listings by key word • Post response to listing on board • Establish communications with lister by following up on contact information in listings using unconnected communications tools 	<ul style="list-style-type: none"> • Operates on private network or over the Internet • Post listing to a board by filling out a form • Listings and responses can have attachments and documents • Display listing summary in a table, with sorting by title, date, market type, buy/sell, or listing number. • Search listings by keyword • Register keywords with an electronic "agent" that monitors listings and sends notice of relevant new listings by Email • Post response to listing on board • Send private response (anonymously or with name attached). • Response can be through a "reply card" designed by the trader posting a listing, to structure responses • Direct connection between listings and communications tool

Analysis	<ul style="list-style-type: none"> • Internet access to research resources, on line and third-party analysis 	<ul style="list-style-type: none"> • Internet access to research resources, on line and third-party analysis • Research resources searchable using the same search engine and display as used for listings. • Online dialogs / user groups
Negotiation	<ul style="list-style-type: none"> • Requires private network • Directory of contact information for all traders • Connection between directory and Email client. • Directory not linked to other components of the system • Anonymous mail application providing for communications between two individuals • Anonymous mail delivered to mail client • No attachments for anonymous mail • No system for central repository of documents 	<ul style="list-style-type: none"> • Works on Internet or private network • Directory of contact information for all traders. • Direct connection between directory and Email client • Direct connection between directory and online conferencing software • Directory linked to listings and document management tool • Anonymous mail application providing for communications between individuals or groups of people working together • Anonymous mail does not require separate Email client software • Anonymous mail supports attachments • Internet-based system for distributions and sharing of documents. • Password and secure has protection for documents.
Closure	<ul style="list-style-type: none"> • Requires private network • Online signature of uploaded document 	<ul style="list-style-type: none"> • Internet or private network • Online signature of uploaded document • Registration / closure of deal through a fill-in form • Provision for digital signature and archiving of all documents associated with a deal

1

2

Referring to FIG. 1B, one aspect of the system within the framework of the

1 negotiation/analysis loop shown in FIG. 1, is the ability to define one or more
2 contracts, for example, in the parlance of the reinsurance trade, "slip sheets." Various
3 members of a group of authorities modify the contract causing it gradually to take a
4 final form that is either rejected as untenable or accepted as a finalized deal. The
5 system exposes various aspects of the contract and attendant documents to the
6 appropriate participants in the transaction, also providing each with a level of
7 authority to add, delete, or modify documents as well as the evolving contract or
8 contracts (assuming there may be various contract templates being discussed). These
9 filters (filter 1 through filter 4, for example), as shown in FIG. 1B, determine the
10 authority of the party (Party 1-Party 4) to modify or see the data object, whether it is
11 a document or a slip sheet. The system combines this system of filters with signature
12 technology for closing the deal; that is, implementing signatures so that an
13 enforceable contract is generated.

14 A deal is like any other data object and once it is defined and entered, it
15 cannot be modified. Elements of the deal can be "signed" such as documents
16 attached to a contract (for example, Contract 1 has documents D1 and D2 attached
17 to (combined with) it. Together these elements, the contract and the attachments,
18 define the deal. Also, the entire deal 245 can be signed using a signature device
19 ("widget") S8. Other documents may relate to a deal but not be attached. These can
20 be viewed using a document manager described further below.

21 Listing System

22 Referring to FIG. 2, a listing screen displays all offers for contracts, for
23 example offer 314, as well as responses to them, for example, response 313. The
24 parameters of the offers and responses to them are shown in columns, the heading of
25 each of which may be selected to sort the listings by that heading, for example
26 heading 315 if clicked would sort by the unique index number for the listing. Notice
27 that the responses (for example, response 313) are shown indented to indicate a series
28 of elements of a dialogue-thread. As indicated, the responses have a "daughter"
29 relationship to the parent listings. That is, listing 314 is a parent and reply 313 is a
30 daughter. The daughters remain in their hierarchical position beneath the parent
31 despite sorting by the column headings. This makes the tabular sort scheme
32 compatible with a threaded display, which is useful to show dialogues.

33 Referring now also to FIG. 3, when a user invokes a display of the details of

1 a listing by clicking on an index hyperlink 312 to show the details of the listing, a
2 user interface element displays the lister's defined parameters of the listing. As
3 shown, various parameters are displayed, many of which are hyperlinked. For
4 example, attachments 304 may be selected to display the corresponding attachments.
5 A detailed description 301 may be provided as well as specific instructions for
6 responding 302. A reply button 303 permits the user to reply. Activating the reply
7 button 303 will either invoke a standard public reply screen which creates a new
8 listing similar to the parent listing or a special reply defined by a reply card which is
9 further described below.

10 A reply to a listing can take the form of a public reply that invokes a screen
11 substantially the same as FIG. 3 but with blank spots for entry of reply information.

12 A more useful kind of response element is a reply card that can be defined by the
13 lister. This is because in negotiations on complex transactions such as reinsurance
14 contracts and, for example, pollution emission allowances, the parties with whom a
15 lister would be willing to trade are limited in terms of certain criteria. These criteria
16 will vary from one type of transaction to another.

17 In an active trading system, the number of listings can quickly grow to a large
18 number and quickly exceed the number which can conveniently be displayed in a
19 single table. Several capabilities are built into the system to address this problem.

20 First, by default, listings are presented in order from newest to oldest. Second, the
21 sort capabilities previously described allow users to modify the standard order.
22 Third, the total market may be divided into subcategories. In the area of insurance
23 catastrophe risk, these could include categories for different lines of insurance (e.g.
24 marine, aviation, commercial buildings). Fourth, users may enter search criteria to
25 identify a subset of listings of particular interest.

26 Searching listings: A user may enter a keyword such as "hurricane" to
27 identify all listings that contain that word in the title, description, and (optionally)
28 attachments. To improve the reliability of the search, users are provided access to
29 a standard lexicon when composing a listing. In the first embodiment, this capability
30 is invoked by pressing the right mouse button while the cursor is any field of the
31 listing. A list of common terms is displayed. The user can select the term of
32 interest, which is then placed into the text of the listing at the insertion point marked
33 by the cursor. For example, a listing for insurance risk would typically include a

1 field for geographic scope (i.e. the location of the properties to be insured). When
2 in this field, the lexicon displayed would include terms such as "California" and
3 "Coastal Florida". Choosing a term from the lexicon insures uniformity of
4 terminology across listings and between the search engine and the listings.
5 "California" will be used rather than a mix of "Ca", "CA", "Calif", etc. The search
6 is further improved by symantic indexing. Essentially, this means that synonymous
7 terms are grouped, so that searches for one will find the other. A person who
8 searches for "California" will get listings for "Los Angeles" that do not include the
9 word "California".

10 The search engine can include an agent capability. This agent capability
11 offers the user the option of saving a search, after the user reviews the results and
12 deems them acceptable. This search is retained in a library of searches along with the
13 email address of the owner of the agent. The search is retained in the library until
14 is it either deleted by the user when it is no longer needed or automatically deleted
15 in a cleanup of searches older than a certain date. Whenever a new listing is placed
16 on the system, all of the saved searches are executed. If the new listing meets any
17 of the search criteria, a message is sent to the owner of that criterion via email or
18 instant messaging.

19 A model was developed to allow a lister to define a set of criteria and request
20 a set of information from any respondents in the form of an anonymous reply "card."
21 The card defines a set of requested information which may be packaged as a
22 document object and placed in the document manager system and connected with
23 each listing. A user would download the reply card and fill the card out and send it
24 back to the posting party.

25 A document object, called a reply card, is made available to a respondent
26 through the document manager. The respondent is permitted to retain his anonymity
27 as is the lister. Each may communicate with the other through an Amail system
28 described in more detail below. The respondent supplies the requested information
29 and sends the data to the lister. A system in the listing manager allows a lister to
30 define a reply card having any particular fields and instructions required of a
31 respondent. Some of the information required may be obtained automatically from
32 a set of default data stored on the respondent's computer.

33 Referring to FIG. 4, a reply card definition screen is invoked to define the

1 parameters of a new listing. The new listing is defined using a user-interface element
2 looking much like FIG. 3. While the details are not critical, the definition of reply
3 card involves, in essence, the definition of a user-interface control such as a dialog
4 with radio buttons, text boxes, etc. These are definable for server-side
5 implementation through HTML and are well known so the details are not discussed
6 here. The lister defines a set of controls that allow the entry by a replying party of
7 the information that the lister requires. The reply card is stored as any other
8 information object and may be organized and accessed through the document
9 manager described below. FIG. 4 shows a simple example of a format of a reply
10 card.

11 A reply card is created by a user when posting a new listing. The lister
12 specifies the information that must be included in a response, and the type of
13 information object to display for the data element (e.g. a text box, check box, radio
14 button). The system then creates an HTML page to collect the requested information.
15 When a respondent clicks "Reply Card" on the listing screen, the page is displayed.
16 All of the responses are automatically entered into a database created automatically
17 when the reply card is composed. As each respondent fills out a reply card, a new
18 record is added to the database of the system and the lister is permitted to view it
19 through an appropriate filter as discussed above.

20 Signature System

21 As business is increasingly done in an electronic environment, electronic
22 signature and approval is becoming more critical. The typical electronic signature
23 model has focused on two aspects:

- 24 1. Electronic validation of the user -- specifically determining that the person
25 viewing a document on line is the authorized signatory; and
- 26 2. Validating the document being signed by a means that either prevents
27 modification of a document or will reveal whether changes have been made.

28 Methods for validation of identity range from simple personal identification
29 numbers or passwords, to electronic signature pads, and more advanced methods of
30 biogenic validation such as fingerprint or retinal patterns. Methods for document
31 validation range from simple archiving of one or more copies in a read-only model
32 or inaccessible location to methods based on mathematical algorithms that create a
33 characteristic number or alphanumeric string for a document. These strings are

1 termed "electronic signatures." Changes to the document change the electronic
2 signatures. Because the signatures are much shorter than the documents, very many
3 documents have precisely the same signature, but the algorithms to calculate the
4 signature are very difficult to invert, so that it is effectively impossible to deduce a
5 meaningful change to a document that will preserve a specific signature.

6 These two aspects of electronic signature are highly developed, but there has
7 been little analysis or development of the general process by which documents can
8 be signed.

9 The invention allows for secure and reliable routing of documents, for which
10 signatures are required, to a specified list of signatories. Unlike prior art systems,
11 such as ordering or accounts payable systems which have highly structured signature
12 procedures tailored to a specific process, the present invention provides a flexible
13 method and system that allows a signature-type of authority/requirement to be
14 attached any kind of information object. The method is sufficiently abstract, flexible,
15 and general that it can be applied in many contexts aside from the CITE embodiment
16 described in the present specification.

17 One signature method/device employs the following steps:

18 1. Registration of signatories – This process provides a register of identifiers
19 indicating entities with signatory authority and correlates these identifiers with the
20 information objects for which the signatory authority is applicable. The same register
21 may also be used to identify other types of authority in the system in which the
22 signature device is implemented. For example, document read authority,
23 modification authority, exclusive access to documents, etc. may also be provided in
24 the same register. Signature registration may be provided automatically in certain
25 systems where registration of, for example, read/write authority is provided since any
26 entity with signatory authority would in almost all instances, also be provided with
27 some other kind of authority, most notably, read authority. Thus, where the signatory
28 system is embedded in certain kinds of systems, it may be that no particular
29 additional method or device is required to implement signatory registration since an
30 existing register may already exist or be required for other purposes.

31 Registration information includes the general categories of information listed
32 below. Definitions of specific fields within these categories are a function of the
33 specific implementation of the signature system or the parent system. The following

1 are exemplary:

2 1. Identity – unique identifier of the entity, the organization(s) with which the
3 entity is affiliated, other relevant information.

4 2. Contact information – information indicating how the entity can be
5 reached, how documents and mail messages can be routed to the entity.

6 3. Security Information – a password for each class of signature as described
7 further below.

8 2. Classes of signatures – The device/method provides a variety of classes of
9 signature, each associated with a unique level of approval or level of commitment.

10 For example, a class of signature-authority can be defined that represents
11 individuals, for example, with authority to sign contracts only below a set amount,
12 or for expenses relating only to one department of an organization, or within certain
13 time constraints, etc. The signatory system maintains this taxonomy of possible
14 signature types in a database with a unique identifier for each level of authority
15 defined. The system allows the creation and deletion of classes. Each class is
16 preferably permitted to be named and a descriptive definition attached to each class.

17 3. Defining a Set of Signatures – Using an appropriate user interface element, the
18 user of the system selects an information object (for example, a document, file, or
19 collection of such objects) requiring signature(s). The entity originating the signature
20 process then identifies the entity or entities required to sign the object. The
21 specification of the signers can proceed either by the selection of individuals from a
22 list supported by the above defined entity register. Alternatively, in an environment
23 where individuals are strongly bound to organizations, for example, it can proceed
24 by selecting the list of organizations that will sign and, within each organization, the
25 person who will sign. The list is built by a series of selections. After each selection
26 from the list, the user indicates his/her desire to add the selected individual to a list
27 of required signatories. The user interfaces provides for entries in which all the
28 selected signatories are required or only one of the selected signatories are required.

29 For example, if more than one entity is selected from the list prior to the
30 selection (e.g., clicking an “Add” button), the system may require a signature from
31 any of the people selected, but not all of them. To require signature from every
32 member of the group, the initiator may select one person, then “add”, select the
33 second, then “add”, and so on. Thus, adding a group with one “add” command would

1 provide an “any signature will suffice” list and adding members individually would
2 require a signature from that individual or entity. Note that this technique may also
3 be used to define combinations of required and “any of” groups.

4 For each signer or group of signers selected in a single “add” command, the
5 initiator of the signing sequence must specify the class of signature associated with
6 the person for the document being signed. This may be selected from a list of
7 signature classes (see item 2). If the specific implementation of the signature process
8 only supports one class of signature, the selection of class may be omitted.

9 4. Random or Serial Order of Signature – After or concurrent with the creation of a
10 signature list, the initiator specifies whether signatures must be in order or if a
11 specific order is not required. For purposes of defining the order of signature,
12 individuals who are selected as a group are considered as occupying a single place
13 in the sequence.

14 5. Document Authentication – Upon initiating a signature sequence, the information
15 object is authenticated by means of a secure hash algorithm. The specific hashing
16 algorithm is a matter of design choice or may be made dependent on a user’s choice.
17 There are several possible hash algorithms available in the public domain. The
18 electronic signature produced by the secure hash algorithm is archived with the
19 information object in a secure repository. If the information object is, for example,
20 a record in a database, the contents of the record are copied to a file in delimited
21 format for archival purposes. If the object is a table, the table is exported prior to
22 archive.

23 6. Document Routing – Upon initiation of a signature sequence, the initiator
24 specifies how the signatories are to be informed. The options are:

- 25 • No notification from the signature system
- 26 • Email message
- 27 • Email message with attachment of the information object.
- 28 • Posting on a signature web site

29 The system accepts and implements the chosen method, which may be connected to
30 the signature or a single choice applied to all signatories. Alternatively, the method
31 of notification may be stored with the signature class definitions. In a signature
32 process with no required order, e-mail notice may be sent simultaneously to all of the

1 designated individuals at the time of initiation. If the process is serial, only the first
2 person may be notified. The electronic signature of the information object may be
3 included in an e-mail message.

4 7. Accessing the signature system – The signature system can be implemented for
5 access via a web browser or database client-server software across the Internet, an
6 intranet, a LAN, or a WAN. Access to the system will typically require a password,
7 but this may not be necessary on a secure network. Upon access to the system a user
8 will have the option to display a list of all of the information objects which he or she
9 has signed or is being asked to sign. For each object, the display can include the
10 following information:

- 11 • Object name
- 12 • Description of object (text, mime, size, date)
- 13 • List of scheduled signatories
- 14 • Date each person signed
- 15 • Class of signature for each person
- 16 • Electronic signature produced by the secure hash algorithm

17 If the object is available (viewable) on line, the display may also include a link to
18 display or download the object.

19 8. Validation of the Object at Time of Signature – If the user downloads or views the
20 object, the system will execute the secure hash algorithm to calculate the electronic
21 signature. This will be displayed so that the potential signer can compare it to the
22 signature calculated at the time the process was initiated. If the user has previously
23 downloaded the object or received it as an attachment to an Email, the user may
24 access the secure hash code through the signature system and apply it to the version
25 on the user's disk.

26 9. Signing a Document – After the user has determined that an information object
27 is authentic and that the contents merit signature, he or she can affix a signature by
28 authenticating his or her identity. Various means of authentication may be used. The
29 means of authentication may be at the discretion of the manager of the signature
30 system. Such means may include personal identification numbers, passwords,
31 authentication based on computer address or information stored on the signer's
32 computer, third party validation using a public key or other security infrastructure,

1 or biogenic (fingerprint-recognition, retina scan) methods.

2 After a document is signed, the date of signature is recorded in a database so
 3 that the display to other potential signers is updated. If the signature process is serial,
 4 the next person in the sequence is notified. E-mail notice can be sent to all signers
 5 when the last signature is collected.

6 10. Follow-up – At the time a signature process is initiated, the initiator can select
 7 a time (in hours, days, or a time or date-certain) for automated follow-up. If a
 8 document is not signed within the specified period after notice, a follow-up e-mail
 9 can be sent as a reminder. Additional reminders may be sent at the same interval if
 10 the object has not been signed. The reminders can be sent automatically by the
 11 system according to user-input specifications.

12 11. Cancellation – The initiator of a signature sequence can modify the sequence at
 13 any time, except that a signer can not be deleted from the list once they have signed
 14 an object.

15 12. Transfer of authority – The individual initiating a sequence can transfer the right
 16 to modify the list signature list to another individual in the system with appropriate
 17 validation of identity.

18 Document Manager

19 Successfully conducting commerce over an electronic network requires the
 20 exchange not only of messages, but of substantial blocks of information in the form
 21 of documents and data. Beyond simply transferring files from hand to hand, it is
 22 often necessary for multiple parties to work on a document simultaneously or
 23 serially, to track changes, and to maintain a record of versions. Two general
 24 architectures have emerged for document management, which can be termed a "mail
 25 model" and a "repository model." Under the mail model, documents are attached to
 26 messages and circulated person to person. Under the repository model, documents
 27 are placed in a central location. There are advantages and disadvantages to each. At
 28 a summary level:

	Mail Model	Repository Model
--	-------------------	-------------------------

Advantages	Precise routing on a document specific basis. Push in the recipient is informed of a new document. Coupling between document flow and a messaging. Dating is automatic.	Compact storage -- only one version of a file need to be stored. Natural group of files on the basis of subject or access group. Supports good configuration management and version control.
Disadvantages	Creates multiple versions of a document, confounding configuration management and version control. Does not easily couple to online collaboration. Many mail servers limit size of attachment. Relatively high effort to prepare messages.	Not push in the sense that users are automatically informed of new documents. Security model is more complicated than for email. Prior arrangement is necessary to access a repository.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

A browser-based document management model and tool combines the best features of repository model and the mail model, for document dissemination and sharing across the Internet or an intranet.

General Architecture – The general architecture of the system combines two basic components: (1) a database of directories and documents and (2) a directory of users.

The directory of documents lists documents (of any type) contained in the system, and folders that can contain documents or other folders. The directory of users contains a list of individuals and organizations that can access the system, with passwords and/or other information necessary to validate identity and to establish authority.

Representation of document – The term “document” is used here in the broadest sense of any file that can be stored magnetically or electronically. Preferably, each file is given a unique name consisting of a string of no more than 256 characters. Preferably, the character set is limited to those members of the ASCII character set

1 which are displayable or printable. Thus, such codes as "escape" which have no
2 visible representation, would be excluded. This is the file name that is displayed for
3 purposes of identifying the document to the users. There is also an actual file name
4 (which is not shown to users) to identify where copies of the file are stored in the
5 central repository. Certain other information is kept in addition to the name of the
6 file. This includes the following:

- 7 1. Data of creation
- 8 2. Date entered into repository
- 9 3. Person who entered the document into the repository
- 10 4. Description
- 11 5. Size of the document
- 12 6. Document type if known
- 13 7. Date of last update
- 14 8. Access password (optional) stored in encrypted form
- 15 9. File folder(s) where the document appears
- 16 10. Actual file name

17 In addition to the above information, data indicating whether the file is
18 checked-out and to what entity, and the identities of entities that have checked the
19 document out and returned it in the past are also stored. The term "checking out" is
20 described further below. These functions related to file change control and
21 configuration management, which are discussed later.

22 User database – A database contains information on all individuals who can currently
23 access the system or who previously had access up to an administratively determined
24 retention period. This database includes standard contact information including
25 physical and electronic addresses. Security data such as passwords and/or encryption
26 keys is also maintained. In a combined system such as the presently described
27 system, the same database or registry of users can be employed for the document
28 manager as for the signature system.

29 High level directories – The entire document management system can be divided into
30 a number of high level directories that the user can display, one at a time. These
31 include, at a minimum, a "Private" directory of files and folders visible only to the
32 user, and a "Public" directory of files and folders visible to all users. Additional
33 high-level directories can be created by the system administrator as needed. These

1 could correspond to projects, business units, or any other logical basis. At any point
2 in the use of the document management system, a user can see and select from the
3 high level directories to which the user has access. The name of the currently open
4 directory can be always displayed on the screen.

5 Displaying the contents of a high-level directory – When a user selects a high-level
6 directory, the repository displays a series of file folders against the left margin of the
7 active window. File folders whose contents are displayed are shown as open folders.
8 File folders whose contents are not displayed are shown as closed folders. A folder is
9 opened or closed by clicking a single time. When a folder is opened, the contents are
10 shown with an indent to indicate the parent/child relationship between the folder and
11 its contents. Each folder can contain files, shown by an icon representing a printed
12 page and other folders, represented by an image of a closed folder.

13 Information about a folder – Information about each folder is displayed on the same
14 line, to the right of the folder icon. This information is as follows, from left to right:

- 15 1. Name of the folder
- 16 2. Number of files in the folder, or the word "empty"
- 17 3. Accessibility of the folder

18 Accessibility refers to user access rights to a folder which may private relative to the
19 entity that created it, restricted (limited to a subset of people who can access the high
20 level directory), or shared (available to everyone with access to the high-level
21 directory). The level of access to a directory is indicated by the words "private",
22 "restricted" or "shared."

23 If the directory is restricted, clicking on the word restricted displays a list of
24 the entities that have access to the folder. This list is a series of hyperlinks. Clicking
25 on the name of a person pulls up detailed contact information (discussed below). The
26 objective is to facilitate communications between people with a shared interest in a
27 file.

28 Information about a file – Information about a file is displayed to the right of the file
29 icon. From left to right, the first item displayed is the name. This is followed by the
30 word "details." Clicking on "details," causes the document management system to
31 display complete information about the file (see Item 2, above), the person who
32 placed the document in the file, (see Item 3, above), and the person who most
33 recently modified the file.

1 Information about people/entities, and the link to communications – Information.
2 about people/entities with access to the system is displayable at several points in the
3 document manager system:

- 4 1. by accessing the directory of users
- 5 2. when creating a new folder with "restricted" access
- 6 3. when displaying detailed information about a file (see #7)
- 7 4. when displaying information about a restricted directory (see #6)

8 Whenever such information is displayed, contact information from the database is
9 rendered along with the name. Depending on the implementation, this can include
10 complete contact info (multiple addresses, telephone and fax numbers, and email
11 addresses), or some of the contact information may be restricted, in which case it is
12 not displayed.

13 Creating a new top level folder – A new folder is created within a high-level
14 directory, for example by clicking a button labeled "new folder." This can bring up
15 a dialog in which the user assigns a name to the new folder and selects the type of
16 access (private, shared, or restricted) rights to be assigned. If the document is
17 restricted, the user specifies the entities (organizations and/or people) that can access
18 the folder. If the creator of the folder specifies that an organization has access to a
19 folder, all individuals associated with that organization may be granted access.
20 Folders to which a user does not have access may remain hidden or not displayed.

21 Alternatively, these folders can be shown with some indication that they are not
22 accessible, for example, by ghosting.

23 Functions related to a folder – Once a folder is defined, a user can execute the
24 following options.

- 25 1. Create a subfolder, using the same process described in 9
- 26 2. Add a document to the folder, using the process described in 11
- 27 3. Delete the folder, if it is empty
- 28 4. Modify access to the folder using the same tools used to specify access
29 initially

30 The functions can be invoked by, for example, clicking on the appropriate label to the
31 right of the name of the folder icon.

32 Adding a file – Users add a document using a dialog box that prompts for the
33 following information:

- 1 1. Location of file - may be entered by user, or selected through a standard
- 2 file browse dialog
- 3 2. Name to be used for the file in the repository
- 4 3. Version number or name (optional)
- 5 4. Password or encryption key (optional)
- 6 5. Description (optional)
- 7 6. Access rules (read only or read-write)

8 After entering the above information, the user either aborts or initiates upload.
9 The information listed above is recorded along with the name of the person entering
10 the document, and date and time.

11 File options - The following functions may be provided, preferably for every file in
12 the system:

- 13 1. Delete (with confirmation)
- 14 2. Archive. The file is removed from main repository, but a copy is retained
15 outside the repository. It may be restored though manual intervention.
- 16 3. View or download: a copy of the file is brought to the user's computer.
17 This file can be modified there for the individual user's use. A modified
18 version can be uploaded as a new file or different version of a current one, but
19 a file in the repository can only be replaced if the user has it checked out.
20 4. Check out / check in (see below)
- 21 5. Forward (see below)
- 22 6. Change Password. The old password must be entered followed by a new
23 password and confirmation.
- 24 7. Move: copy or move a document from one folder to another.

25 The functions may be invoked, for example by clicking on a label
26 corresponding to the function, which can be displayed to the right of the name of the
27 file. Not all options are shown to all users. If an entity does not have write-access
28 to a file, the entity may not delete it, archive it, check it in or out, or change the
29 password.

30 Check in / Check Out - All entities with write access to a file may check it out. By
31 checking the file out, the entity reserves the exclusive write to save changes to a file.

32 A person may not replace a file that is checked out. To check out a file, the user
33 selects this option from the list of functions associated with the file. The user can

1 then enter an expected return date and a reason that the file is checked out or the
2 changes to be made. This information is available to all others who can view the file.
3 Each check in or check out is recorded in a permanent log. After a file is checked
4 out, the "check out" button or link is changed to read "check in."

5 Each individual can check in only the files that he or she has checked out.
6 This is done by clicking "check in." The user may then upload a new version of the
7 file by specifying the location of the file on disk, or indicate that the version of the
8 file currently in the repository is to be retained. After a file is checked in, the check
9 button is changed back to "check out" and the file can be checked out by another
10 user.

11 Forwarding – A file can be forwarded to any other user of the system. When the
12 forward function is invoked, a list of users is displayed. The sender selects one or
13 more users. Upon confirmation, a copy of the document is placed in folder labeled
14 "in box" in each recipients private directory.

15 Referring to FIG. 5, a main screen for the document manager creates (using
16 server-side scripting) a user-interface display with some of the features of a Windows
17 Explorer® -type display. File and folder icons are shown along with an array
18 features arranged next to each. The similarities with Windows Explorer® fairly well
19 end there, however. Each of the properties shown next to each file/folder entry
20 invokes a feature.

21 A parameter object W "Details" invokes a detailed display of the
22 corresponding document object. The details can include contact information about
23 the creator of poster of the document or other data as desired. This data can be
24 hyperlinked and a return button can be provided to return the display back to the
25 screen shown in FIG. 5. Clicking the "details" button to the right of any document
26 brings up the display which can include the name, contact information, and other
27 details about the person who loaded the document into the system, similar
28 information about a person who has the document checked out, and, optionally, a
29 description of the document and information on its change history.

30 A parameter object X "Forward" simply sends the document to a selected
31 user. A selection screen can be invoked to allow selection of the recipient of the
32 document from the user registry. Of course, since most correspondence can be
33 handled on the server side, the user is, in reality, simply notified of the transfer and

1 the recipient's action to view the document simply invokes a server side feature to
2 display the document. The document is not actually transferred bodily to the
3 recipient since the recipient, as a registrant logged in the user registry, can access it
4 through the server by requesting to do so.

5 A parameter object U "Check-in" checks in a document that has been checked
6 out. Other users may view the document, but not modify it when it is checked out.

7 This button is not accessible to users that have not checked the document out and
8 may be displayed ghosted or not displayed at all. A similar button can be displayed
9 if a document that is not checked out may be checked out by the user authorized to
10 see the document manager displayed shown in FIG. 5.

11 A parameter object T "Download" actually transfers a copy of the document
12 to the client computer. Another object S "Delete" allows the document to be deleted.
13 A new document can be added by clicking "New Document" Q. These are fairly
14 conventional notions, except for their placement on the screen and the fact that each
15 is filtered depending on the user's rights.

16 Note that when a folder is created, access to the folder can be restricted to the
17 creator, shared with everyone (in which case the folder is created in the public
18 directory), or shared with a select group of other users. The other users can be
19 selected by company or organization (providing access to all individuals in the
20 organization) or by individual within an organization. These are all selectable
21 through a linked selection control where if one selects a company in one selection
22 control, it shows employees in the linked selection control.

23 A parameter object P "Shared" displays a hyperlinked page that shows all
24 users with access rights to the document. This page allows a user that places a
25 document in the document manager or a user that has pertinent modify rights, to alter
26 the parties that have access to the document. Also, it allows a user with read-only
27 rights to see the list of users that can access that document. The names of the sharing
28 parties are hyperlinked to invoke the user's email client to allow fast sending of email
29 (which again may be performed server-side without actual transfer) or conventionally
30 or selectively. If a folder is shared, the word "Shared" appears to the right of the
31 folder. Clicking on "Shared" brings up the list of person who can access the folder,
32 as shown in FIG. 6. Each name is a hyperlink to detailed contact information.

33 FIG. 7 shows a list of all deals that were completed through the system. The

1 trade number (left column of the grid) is a hyper link to detailed information.

2 FIG. 8A shows detailed information about a completed trade. It shows the
3 party to the trade, the price or rate, and a description of what was traded. The
4 particular nomenclature is specific to a market. For insurance, for example, price is
5 termed rate, and the summary of a deal is the slip sheet. A complete contract can be
6 attached. Included documents can be downloaded to view on line. The intended
7 signatories to a deal are shown (there can be more than two).

8 If a signatory has actually signed the document electronically, the date and
9 time are shown. No date and time are shown for parties that have not yet signed.

10 The amount of information displayed on the screen is dependent on the identity of
11 the person viewing the screen. The viewer can be blocked from viewing any
12 information about a deal, or certain fields, such as the contract details or the name of
13 signatories.

14 Note that the detail screen of FIG. 8A would also show attached exhibits. The
15 FIG. 8A display is the basic device for signing deals. A similar device would be used
16 for signing documents.

17 Referring to FIG. 8B, all of the information necessary to document a deal is
18 pulled together through the screen below. The deal summary includes highly
19 structured information on parties, dates, terms, etc., as well as unstructured
20 information in the form of attachments. The bottom part of the page allows the
21 person registering the deal to designate the intended signatories. When the signers
22 affix their electronic signature, they are doing so to all of the documents in the deal,
23 including the attachments. These are archived and protected from tampering using
24 secure hash technology. In this way it is possible to create a reliable, on line
25 electronic signature to a complex deal, without risk of repudiation.

26 Note that any number of exhibits can be added to the UI device of FIG. 8B
27 since the list scrolls from the bottom each time a second exhibit is added. The user
28 interface has self-explanatory elements for defining information about the deal.

29 Anonymous Mail

30 For purposes of the following description, a "subscriber" is a person or entity
31 that subscribes to an anonymous mail system to be described below. Certain types
32 of negotiations and communications require anonymous initial contact, followed by
33 some period of anonymous discourse, leading to eventual disclosure of the parties'

1 identities. In the course of a typical sale or business deal, the initiating party begins
 2 either by contacting one or more targeted potential trading partners or advertising to
 3 a community of potential partners. While the identity of the initial offeror is usually
 4 clear in any direct contact, it need not be so in advertising. In certain cases it could
 5 be problematic for the initiating party to reveal his or her identity:

6 A party to a deal can have difficulty controlling the method of contact once
 7 the party's identity is known. If a company is known to be in the market for office
 8 space, for example, the party may be subjected to badgering by real estate firms
 9 outside the established bidding process. Executives of the company may be contacted
 10 directly in an effort to influence the decision.

11 Disclosure of intent may adversely affect the market. If a large company
 12 begins to acquire land in an area, the price can rise very quickly. Simple exploration
 13 of an option can make the option more costly or even impossible.

14 Disclosure of intent may adversely impact the reputation or standing of a
 15 company. An insurance company that determines that it is over exposed to a certain
 16 peril (e.g. hurricane losses in the Southeastern U.S.) would reveal that situation to
 17 their competitors and investors by a large public solicitation.

18 While anonymity can be crucial for the initiator of a deal, it can be equally
 19 important for the respondent for the same reasons. The need for controlled anonymity
 20 has been addressed by several methods that were initially developed for paper
 21 communications and have been extended to analogues in telephonic and computer
 22 communications.

- 23 • Numbered mail boxes, including government and private
- 24 • Communications through a mediator
- 25 • Anonymous voice mail drops
- 26 • The use of pseudonyms in computer e-mail and dialogs.

27 These methods have several serious shortcomings:

- 28 • The method may only allow anonymity from one side.
- 29 • There is no inherent mechanism to validate the credentials and intent
 30 on an anonymous party
- 31 • Use of a pseudonym may invalidate its future use by associating the
 32 name with a specific party

- 1 • Manually mediated communications are slow
- 2 • The creation and deletion of pseudonyms may not be completely
- 3 within the control of the party, imposing an overhead cost (in cash or labor)
- 4 and/or delay in creating a new name
- 5 • In most systems, a person with multiple pseudonymous mailboxes or
- 6 e-mail addresses will receive communications in several different places
- 7 (mailboxes or accounts), thus requiring multiple logons/passwords.
- 8 • Routing of messages received anonymously requires manual
- 9 forwarding to all relevant parties by the individual with access to the
- 10 anonymous mail box or email account.
- 11 • There is no mechanism to reveal actual identities in a secure and
- 12 mutually acceptable way.

13 The present invention addresses these deficiencies by providing two-way
 14 anonymous communications, a central point of collection for messages sent to
 15 multiple pseudonymous addresses, connection of multiple parties to a single
 16 anonymous account, and a mechanism to reveal identities to all parties to a deal
 17 simultaneously, by mutual consent. In summary, the anonymous mail system is a
 18 server side system that allows clients to create anonymous handles on the fly. It also
 19 allows them to share anonymous handles among multiple recipients so that the group
 20 of recipients appears as a single recipient to the sender using the anonymous handle.
 21 It is like a transparent mailing group. When mail is sent to an anonymous handle, it
 22 is sent to all members of the group.

23 Multiple Systems – In contrast to the first-generation anonymous mail system, the
 24 present system allows for multiple anonymous mail (Amail) systems. Each Amail
 25 system operates in association with a conventional e-mail server, and uses the e-mail
 26 server for communications with non-subscribers, subscribers to Amail systems other
 27 than the local one, and for forwarding messages to the subscribers Email client
 28 software.

29 Registration – Subscribers to an anonymous mail system (Amail) each complete a
 30 registration that provides:

- 31 • Contact information (name, address, telephone number, fax, etc.)
- 32 • Information to determine whether they the party is qualified to

1 participate in the communications exchange. For example, if the system were
2 to be used between and among real-estate agents, registrants to the system
3 might be required to supply a real estate license number.

- 4 • Association with an organization (if appropriate)
- 5 • Additional information on the individual or organization that may be
6 of use to others in the Amail system to determine the suitability of the party
7 as a partner in negotiations.

8 The additional information can include such factors as credit ratings, assets, or the
9 region in which the company does business. The specific information required
10 depends on the application. Insurance, real estate, energy marketing, etc. would all
11 have different data of interest.

12 Validation – Depending on the business model and role of the organization operating
13 the Amail exchange, the organization can either accept the information provided by
14 the subscriber, or verify the information and provide verification as part of the
15 service. Upon acceptance of a subscription applications and validation of the
16 background information if necessary, the use is assigned an Amail user ID and
17 password.

18 In the first version of the Amail system, logon was automatic from the general
19 application (CATEX); there was no separate user ID and password. In alternative
20 versions, the Amail system can provide its own user ID and password, with the
21 ability to bypass logon when it accessed from other applications with acceptable user
22 validation. All of the actual contact information and validation information are
23 maintained in a database. Validation information was not provided in the first
24 version of CATEX.

25 Assignment of an Email address – Each subscriber must provide an Internet
26 accessible Email address or be assigned an e-mail address in the Amail system. The
27 first version of the Amail required that the user have an Email address on the system.

28 The new version works directly with e-mail systems other than the Amail.

29 Logon – Subscribers access the Amail system by connecting an Amail web page
30 provided either over the Internet or on an Intranet. The subscriber enters a user name
31 and password. The first version of Amail was not browser-based and worked only
32 over a LAN or WAN, not over the Internet or an intranet.

1 Available functions – After logon, the subscriber can access the following functions:

- 2 • Manage aliases
- 3 • Compose an anonymous message
- 4 • Read Amail messages. In the original CATEX system, the user could
- 5 not access messages from within the Amail application.
- 6 • Log off

7 Managing Aliases – Aliases are directly under user control. After logon, a user can:

- 8 • Add a new aliases
- 9 • Delete an existing alias
- 10 • Create a free-form note associated with a new alias, or edit the note for an
- 11 existing alias that will be accessible to recipients from the alias.
- 12 • Identify other subscribers to whom messages to alias should be forwarded
- 13 • Identify other subscribers with permission to generate messages from the alias

14 These last two features make it possible for a group of subscribers to share an alias,
15 allowing them share communications and work together more effectively. The user
16 will:

17 Compose an anonymous message – After logon, a user can create and send an
18 anonymous message. After the option is selected, the system will display a message
19 creation screen with the following features:

- 20 1. A list of aliases currently owned by the user (i.e. created by the user and
21 not deleted), for the user to select the alias from which the message will
22 originate.
- 23 2. A subject box for the mail.
- 24 3. A list of the e-mail and alias addresses to which messages can be sent for
25 the user to select one or more. The original version could only send to one
26 alias. The user can also supply an Internet e-mail address off system.
- 27 4. A list of the e-mail and alias addresses to which copies of the messages
28 can be sent for the user to select one or more. The user may also supply an
29 Internet e-mail address off system. The original version did not include a
30 “CC” feature.
- 31 5. A space where the message can be typed, allowing for users to paste text
32 copies form another system using the Windows-based clipboard utility.

1 6. A check box to select whether the sender is willing to reveal his identify
2 to the recipient on mutual consent.

3 7. A check box to select whether the copies of the message should be sent to
4 other subscribers who share the Alias. The original version allowed only one
5 subscriber to access an alias.

6 Delivery of Messages – After an Amail message has been composed (see step 7), it
7 is delivered as follows.

8 1. The body of the email message is modified by adding a header including
9 routing information and an indication of whether the sender is willing to reveal
10 identities if there is reciprocal concurrence. The message would appear as shown
11 below. The items in italics are new since the original (prior art) version. The first
12 generation of the anonymous mail system did not allow for communications between
13 multiple Amail systems and, hence, did not list the Amail system name in the list of
14 respondents. The first generation system also did not allow for multiple recipients.

1
2
3
4
5
6
7

This message was sent anonymously from alias: Amail system name: alias
The message was sent to:
Amail system name: *alias*
Amail system name: *alias (cc)*
Amail system name: *alias*
The sender is willing to reveal identities.
[Original body of the message]

8 2. If the message is sent to a specific, non-anonymous e-mail address, Amail
9 composes and transmits a standard Email message. The sender is listed as
10 "amailedmin.alias@xxxxx" where "xxxxx" is the address of the standard mail server
11 supporting the mail system. Off-system access was not a feature of the first version.

12 3. If a message is sent to an alias on the local or any other related Amail
13 system, and the owner of the alias has an off system email address, a message is sent
14 as in step 1, above. In addition, however, the message is stored in an Amail message
15 database for access through the Amail system interface. The original version did not
16 have an Amail message database.

17 4. If a message has been sent to an alias for which there is no associated
18 conventional mail account, the message is stored in the Amail message database. The
19 Amail message database contains a repository for all messages, listing the
20 subscriber(s) associated with the alias to which the message was addressed. The
21 database contains the message (including sender, addressees, and ccs), date and time
22 of transmission, and the alias of the subscriber to which the message was sent. The
23 original version did not have an Amail message database.

24 5. If the option was checked to send copies to other that share the alias (see
25 above), copies of the message are placed in the message database for the subscribers
26 associated with each of the aliases.

27 Receipt of Messages – Messages sent from the Amail system can be received in a
28 standard e-mail client by Amail subscribers and non-subscribers.

29 Amail subscribers can also receive messages through an Amail reader
30 interface. All messages received are placed in the Amail message database (see
31 above). Since an alias can be associated with more than one subscriber, the Amail
32 message database can list more than one subscriber as an "owner" of the message
33 even if it was sent to only one alias. When a user logs on and selects the option to

1 read Amail messages (see above) the messages are rendered as an HTML page
2 through a browser. Messages to all of the aliases associated with the user are
3 displayed. Each message has a hotlink to respond to send a message back to the
4 sending alias. Each message also has a link to display the background and validation
5 information and note associated with the alias (see above). The original version did
6 not provide an Amail viewer nor did it provide for display of validation information.
7 Responding from off System from Amail – Individuals from off system can respond
8 to Amail messages using the standard reply feature of their mail server. Messages
9 will be returned to the reply address (see above). Messages received by the
10 conventional e-mail server supporting the Amail system will forward the message to
11 the Amail message repository for the alias listed in the return address. Responding
12 from a standard Email client was not provided in the original version.

13 Flip Widget

14 Increasingly, computer applications are delivered through browsers over the
15 Internet or an intranet. There are many design considerations in building a system
16 for browser delivery in contrast to delivery as conventional client server application.
17 Two related considerations are the graphic richness of a browser screen and the time
18 lag to render a new screen. Partly because good web pages contain complex graphics
19 and partly because the Internet can be a relatively slow network, it is important to
20 design a web application to make few unnecessary wholesale screen changes. It is
21 more economical from the perspective of data transmission and, hence, from response
22 time, to create a “flat” rather than “deep” hierarchy of screens, and change only the
23 part of a screen that is minimally necessary.

24 For example, it is better in a data query to provide a single screen that allows
25 a user to specify a state and city within the state than to provide a first screen for the
26 state, followed by a second screen for the city. As the function of screens becomes
27 more complex, however, it becomes an increasingly difficult challenge to fit all of
28 the options onto the screen (particularly when a user selects a lower screen
29 resolution) and while maintaining a clean appearance. The invention described here
30 provides a tool that allows the Internet application developer to display an effectively
31 unlimited number of options in a very small space using a very familiar and intuitive
32 display feature.

33 Appearance – The “Flip Widget” tool renders a graphical object representing two

1 rows of file folders, overlapping. The labels on the front row are visible, the labels
2 on the second row are obscured by the front row of tabs, but the edges of the apparent
3 back tabs are visible. The number of the apparent tabs displayed in each row is a
4 function of the screen resolution and the length of the longest label entered by the
5 user.

6 The Flip Tab – In one embodiment, the rightmost tab on the front row is labeled
7 “FLIP”. When a user actuates this tab, the response is as described below.

8 Database of labels and links – In creating the display, the application programmer
9 enters a set of paired values. Each pair consists of (1) text of the label to be displayed
10 and a tab, and (2) the name of an HTML link, either within or external to the page to
11 be rendered when the tab is selected.

12 Action – Upon rendering a page containing the flip widget, the two-row tab display
13 shows the first “n” options from the list of labels and links. The value of “n”
14 represents the maximum number that can be displayed while allowing room for the
15 flip tab. Upon clicking any of these tabs, the corresponding link is executed. Upon
16 clicking the flip tab, the two-row tab display is changed to reflect the next “n” options
17 from the list of labels and links, retaining the flip tab on the right. If there are fewer
18 than n options remaining, the flip widget will either display the last n options, or
19 whatever number remain supplement by as many options are needed from the start
20 of the list. Clicking the flip tab when the list has been completed starts the cycle over
21 again with the first option.

22 Referring to FIGS. 9 and 10, a flip widget in a first state is shown in FIG. 9.
23 In the first state, any of the tabs A through E can be selected and the corresponding
24 set of controls displayed. For example, in FIG. 9, tab B has been selected and the
25 controls 430-432 are displayed. If the flip tab 410 is selected, a next row of tabs is
26 brought forward so that the display appears as in FIG. 10 with tabs F through J
27 showing. In FIG. 10, tab G has been selected and the corresponding controls 435-
28 437 are displayed.

29 FIGs. 9A and 10A show a more detailed example of how a flip widget can be
30 used to organize functions available to a user. For example, suppose that one
31 application is a commodity futures trading system that permits a user to execute
32 trades, review prices, and obtain other information relating to various metals such as
33 gold, silver, and platinum. As shown in FIG. 9A, for example, controls or functions

1 430, 431, and 432 (e.g., execute a trade, review current prices, and the like) are
2 associated with a "gold" category and can be invoked easily when that category is at
3 the forefront of the flip widget as shown. Clicking one of the other tabs (e.g., silver
4 tab 400) would bring the functions associated with that category to the forefront
5 while allowing the user to readily select other categories visible behind the front.
6 Clicking "other markets" tab 410 would change the selection of front-row tabs to a
7 different set of categories, as shown in FIG. 10A. The "other markets" tab 410 could
8 be continually clicked to rotate through a plurality of groupings of markets, each
9 having a set of functions or controls associated therewith.

10 A flip widget can be implemented in conjunction with the first or second
11 embodiments of the present invention in order to permit many different functions to
12 be displayed in a small screen space. The flip widget is a device to organize many
13 different functions in a logical way, and can be used as a tool for building an interface
14 to multiple applications. As one example, in a DCE (described in more detail
15 below), there may exist n functions (e.g. bulletin boards, chat rooms, e-mail, a-mail,
16 transaction engines, and the like) the specific availability of which can be defined by
17 a user who creates the collaborative environment. This collection can change over
18 time. Accordingly, the interface cannot be "hard coded" for a particular user.

19 One way to represent an indefinite (and potentially large) number of functions
20 in a small space is with tabs resembling a file folder, with a graphic element
21 representing hidden cards, implying that the user can reach the functionality on the
22 cards by paging (i.e. flipping) to them. The flip widget makes it possible to provide
23 a link to a list of applications maintained in a database rather than requiring that they
24 be hard coded. Programming logic for storing folder labels in a database, linking
25 those labels with associated functions and activating them using browser-type
26 buttons, and for performing the display features described above, are conventional
27 and no further elaboration is necessary. Although the "flip widget" provides one
28 method of structuring a user interface to structure a user's view of application
29 functions, other methods can of course be used.

30 B. DYNAMIC COLLABORATIVE ENVIRONMENT EMBODIMENT

31 In a second embodiment of the invention, a dynamic, user-defined
32 collaborative environment can be created in accordance with a set of tools and
33 method steps. As explained previously, this system differs significantly from

1 conventional networked environments in that: (1) the environment (including access
2 and features) is user-defined, rather than centrally defined by a system administrator;
3 (2) each environment can be easily destroyed after completion of its intended
4 purpose; (3) users can specify a group of participants entitled to use the environment
5 and can define services available to those participants, including offering
6 participation to unknown potential users; (4) the networked environment (including
7 access features and facilities) can cross corporate and other physical boundaries; and
8 (5) the environment offers a broad selection of tools that are oriented to
9 communication, research, analysis, interaction, and deal-making among potential
10 group members. Moreover, in a preferred embodiment, the environment is
11 implemented using web browser technology, which allows functions to be provided
12 with a minimum of programming and facilities communication over the Internet.

13 FIG. 11 shows various method steps that can be carried out to define, create,
14 and destroy an environment according to a second embodiment of the invention. The
15 term "environment" as used herein refers to a group of individuals (or computers,
16 corporations, or similar entities) and a set of functions available for use by that group
17 when they are operating within the environment. It is of course possible for one
18 individual to have access to more than one environment, and for the same functions
19 to be available to different groups of people in different environments.

20 The process of creating a collaborative environment involves the migration
21 of tools and information resources available in the library of the environment
22 generator into a specific collaborative environment. The collaborative
23 environment can include / link to any application available to the environment
24 generator. It can also include applications specific to the environment provided
25 that these are accessible through Internet protocols.

26 Underlying the environment is a directory of users, information about
27 users, and their authorities. The core structure for the environment user database
28 should conform to a directory standard – typically DAP (Directory Access
29 Protocol) or LDAP (the lightweight directory access protocol). The environment
30 generator has access to its own directory of users and to the user directories of the
31 environments it has generated. The directory of an environment can be populated
32 initially by selecting users from the environment generator's directories. These
33 are added to the directory of the environment in one of two ways depending on the

1 specific implementation. Directory records can be copied from the environment
2 generators user database to a separate database for the environment or a flag can
3 be added to the user data record in the environment generators users database to
4 indicate that the user has access to the environment. The second, simple model is
5 useful when all users in an environment have equal authority. A separate user
6 database (directory) is necessary for an environment when the environment has its
7 own security / authority model.

8 Additional members can be added through a set of standard application /
9 subscription routines. These then become known to the environment generator (as
10 well as the specific environment) providing the foundation for greater speed and
11 efficiency in creating subsequent environment.

12 Beginning in step 1101, a new group is created by identifying it (i.e., giving
13 it a name, such as "West High School Research Project," and describing it (e.g.,
14 providing a description of its purpose). The process of creating a group and defining
15 functions to be associated with the group can be performed by a user having access
16 to the system without the need for system administrator or other similar special
17 privileges (e.g., file protection privileges, adding/deleting application program
18 privileges, etc.). In this respect, environments are, according to preferred
19 embodiments, completely user-defined according to an easy-to-use set of browser-
20 driven user input screens. The principles described herein are thus quite different
21 from conventional systems in which a central system administrator in a local area
22 network can define "groups" of e-mail participants, and can install application
23 programs such as spreadsheets, word processing packages, and the like on each
24 computer connected to the network. Moreover, according to various preferred
25 embodiments, the facilities provided to group members can be provided through a
26 web-based interface, thus avoiding the need to install software packages on a user's
27 computer.

28 It is also contemplated that various methods of obtaining payment for creating
29 or joining groups can be provided. For example, when a new environment or group
30 is created, the person or entity creating the group can be charged a fixed fee with
31 payment made by credit card or other means. Alternatively, a service fee can be
32 imposed based on the number of members that join, the specific functions made
33 available to the group, or a combination of these. Moreover, fees could be charged

1 to members that join the group. The amount of the fee could also be based on the
2 length of time that the environment exists or is used.

3 Although not specifically shown in FIG. 11, step 1101 can include the step
4 of creating a new entry in a database table (e.g., a relational or object-oriented
5 database) to store information concerning the new group and the environment in
6 which the group will operate. Database entries related to the group, including some
7 or all of the information described below, can be created as the environment is
8 defined. It is assumed that one or more computers are linked over a network as
9 described in more detail below in order to permit the environment to be created, used,
10 and destroyed, and that a database exists on one or more of these computers to store
11 information concerning the environment.

12 In step 1102, the group members are identified. According to various
13 embodiments, the group members can be identified in three different ways (or
14 combinations thereof), as indicated by sub-steps 1102a, 1102b, and 1102c in FIG. 11.
15 It is contemplated that group members can span physical networks and computer
16 systems, such as the Internet. Consequently, group members can include employees
17 of different corporations, government agencies, and the like. In contrast to
18 conventional virtual private networks, both the group members and the functions
19 made available to those group members are entirely user-selected, thus permitting a
20 broad range of persons to easily create, use, and destroy virtual private networks and
21 associated functionality.

22 First, in step 1102a, group members can be identified by selecting them from
23 a list of known users that are to be included in the group. For example, within a
24 corporation or similar entity, a list of internal e-mail addresses can be provided, or
25 an electronic version of a phone list or other employee list can be provided. If the
26 hosting computer system is associated with a school, then a list of students having
27 accounts on the computer (or those in other schools that are known or connected to
28 the host) can be provided. From outside a corporate entity, users can be selected
29 based on their e-mail addresses (e.g., by specifying e-mail addresses that are
30 accessible over the Internet or a private or virtually private network). In this step, the
31 environment creator specifies or compels group members to belong to the group.

32 Second, in step 1102b, group members can be invited to join the group by
33 composing an invitation that accomplishes that purpose. For example, a group

1 creator may choose to send an invitation via e-mail to all members of the corporation,
2 or all members of a particular department within the corporation, all students in a
3 school or region, or members of a previously defined group (e.g., the accounting
4 department, or all students in a particular teacher's class). The invitation would
5 typically identify the purpose of the group and provide a button, hyperlink, or other
6 facility that allows those receiving the invitation to accept or decline participation in
7 the group. As those invited to join the group accept participation, their responses can
8 be stored in a database to add to those members already in the group. Invitations
9 could have an expiration date or time after which they would no longer be accepted.
10 As invitees join the group, the group creator can be automatically notified via e-mail
11 of their participation.

12 Third, in step 1102c, group members can be solicited by way of an
13 advertisement that is sent via e-mail, banner advertisement on a web site, or the like.
14 Persons that see the advertisement can click on it to join the group. It is also possible
15 for advertisements to have a time limit, such that after a predetermined time period
16 no more responses will be accepted. The primary difference between advertising
17 participation in a group and inviting participation in a group is that invitations are
18 sent to known entities or groups, while advertisements are displayed to potentially
19 unknown persons or groups.

20 It will be appreciated that group members can be selected using combinations
21 of steps 1102a, 1102b, and 1102c. For example, some group members can be
22 directly selected from a list, while others are solicited by way of invitation to
23 specifically identified invitees, and yet others are solicited by way of an
24 advertisement made available to unknown entities.

25 In step 1103, the functions to be made available to the group are selected. For
26 example, the group can be provided with access to an auction transaction engine; a
27 survey tool; research tools; newswires or news reports; publication tools; blackboard
28 facilities; videoconferencing facilities; and bid-and-proposal packages. Further
29 details of these facilities and tools are provided herein. The group creator selects
30 from among these functions, preferably by way of an easy-to-use web browser
31 interface, and these choices are stored in a database and associated with the group
32 members. Additionally, the group creator can specify links to other web-based or
33 network-based applications that are not included in the list by specifying a web site

1 address, executable file location, or the like. The group creator can also define shared
2 data libraries that will be accessible to group members.

3 In step 1104, the environment is created (which can include the step of
4 generating a web page corresponding to the group and providing user interface
5 selection facilities such as buttons, pull-down menus or the like) to permit group
6 members to activate the functions selected for the group. In some embodiments,
7 access to the group may require authentication, such as a user identifier and password
8 that acts as a gateway to a web page on which the environment is provided. Other
9 techniques for ensuring that only group members access the group functions and
10 shared information can also be provided. A web page can be hosted on a central
11 computer at an address that is then broadcast to all members of the group, allowing
12 them to easily find the environment.

13 In step 1105, group members collaborate and communicate with one another
14 using the facilities and resources (e.g., shared data) available to group members. In
15 the example provided above, for example, a group of high school students
16 collaborating on a school research project could advertise for survey participants;
17 conduct an on-line survey; compile the results; communicate the results among the
18 group members; brainstorm about the results using various brainstorming tools;
19 conduct a videoconference including group members at various physical locations;
20 compile a report summarizing the results and exchange drafts of the report; and
21 publish the report on a web site, where it could optionally be offered for sale through
22 the use of an on-line catalog transaction engine. The group could even contact a
23 book publisher and negotiate a contract to publish the report in book form using bid
24 and proposal tools as described herein.

25 In step 1106, after the environment is no longer needed, it can be destroyed
26 by the person or entity that created the group. Again, in contrast to conventional
27 systems, the destruction of the environment is preferably controlled entirely by the
28 user that created the environment, not a system administrator or other person that has
29 special system privileges. Destruction of the environment would typically entail
30 deleting group entries from the database so that they are no longer accessible.

31 FIG. 12 shows one possible system architecture for implementing the steps
32 described above. As shown in FIG. 12, an Internet Protocol-accessible web server
33 1201 is coupled through a firewall 1202 to the Internet 1203. The web server includes

1 an environment generator 1201a which can comprise a computer program that
2 generates user-defined environments as described above. Further details of this
3 computer program are provided herein with reference to FIG. 21.

4 Web server 1201 can include an associated system administrator terminal
5 1204, one or more CD-ROM archives 1205 for retaining permanent copies of files;
6 disk drives 1206 for storing files; a database server 1207 for storing relational or
7 object-oriented databases, including databases that define a plurality of user-
8 controlled environments; a mail server 1208; and one or more application servers
9 1209 that can host application programs that implement the tools in each
10 environment. Web server 1201 can also be coupled to an intranet 1210 using IP-
11 compatible interfaces. Intranet 1210 can in turn be coupled to other application
12 servers 1211 and one or more user computers 1212 from which users can create,
13 participate in, and destroy environments as described herein, preferably using
14 standard web browsers and IP interfaces. Web server 1201 can also be coupled to
15 other user computers 1217 through the Internet 1203; to additional application
16 servers 1215 through another firewall 1216; and to another IP-accessible web server
17 1213 through a firewall 1214.

18 It will be appreciated that the system architecture shown in FIG. 12 is only
19 one possible approach for providing a physically networked system in which user-
20 defined network environments can be created and destroyed in accordance with the
21 principles of the present invention. It is contemplated that application programs that
22 provide tools used in a particular user-defined environment can be located on web
23 server 1201, on user computers 1217, on application servers 1215, on application
24 servers 1209, on application servers 1211, or on any other computer that provides
25 communication facilities for communicating with web server 1201. It will also be
26 appreciated that web pages that provide access to each user-defined environment
27 need not physically reside on web server 1201, but could instead be hosted on any
28 of various computers shown in FIG. 12, or elsewhere.

29 Reference will now be made to exemplary steps and user interfaces that can
30 be used to carry out various principles of the invention, including steps of creating
31 a group, selecting group members, and defining functions to be made available to
32 group members in the environment.

33 FIGS. 13A through 13C show one possible user interface for creating a group

1 and identifying group members. In FIG. 13A, a user gains access to an environment
2 creation tool by way of an authentication process. This may be a simple username
3 and password device as shown in FIG. 13A, or it could be some other mechanism
4 intended to verify that the user has access to the environment creation tool. In the
5 case of a corporation, school, or other entity that already provides a log-in procedure
6 to access the entity's network, such log-in procedure could serve to authenticate the
7 user for the purpose of creating a new environment. It should be appreciated that
8 user authentication is not essential to carrying out the inventive principles.
9 Moreover, although it is contemplated that for ease of use (and to minimize
10 programming) web browsers and web pages be used to receive user-defined
11 information to create each environment, other approaches are of course possible.

12 In FIG. 13B, the user is prompted to create a new group by supplying a group
13 name (e.g., "Joe's Homework") and a brief description of the group. This
14 information is preferably stored in a database file and associated with group members
15 and functions available to those group members.

16 In FIG. 13C, the user is prompted to identify group members. As described
17 previously, group members are preferably identified in one of three ways (or
18 combinations of these): (1) selection from a list of known group members; (2)
19 inviting known candidates to join the group; or (3) advertising for new members.
20 When the user clicks one of the options in FIG. 13C, he or she is prompted to supply
21 additional information as shown in FIGS. 14A through 14C.

22 Beginning with FIG. 14A, for example, group members can be individually
23 specified by entering an e-mail address (e.g., an internal or external e-mail address)
24 in a text form data entry region and/or by selecting from a previously known list.
25 This screen permits the user to compel attendance in the group by specifying names
26 and/or e-mail addresses to which group messages will be sent. All those added to the
27 group in this manner will be provided with access to the environment corresponding
28 to the group. Aliases and pre-defined groups could also be specified as the basis for
29 membership (e.g., all those in the accounting department of a corporation, or all
30 students in a high school).

31 Each member of a group might have a group email account, or they may use
32 an off-system email account. Off-system email addresses can be maintained in a
33 database of users. Mail sent to the group email address is preferably forwarded off-

1 system, protecting the actual email address of the person unless that person wishes
2 to give out that address. New members can be added until the group is completed.

3 Although not explicitly shown in FIG. 14A, it is contemplated that new members
4 can be added to a previously defined group after the environment has already been
5 created.

6 When group members are selected or specified, the user creating the
7 environment can also create a password for each user in the group in order to enable
8 those in the group to access the environment. Alternatively, when a user visits the
9 environment, the environment can retrieve a "cookie" from the user's computer to
10 determine whether the user is authorized to access the environment. If no cookie is
11 available, the user could be prompted to supply certain authentication information
12 (e.g., the company for whom he or she works, etc.) In yet another approach,
13 authentication could occur by way of e-mail address (i.e., when the user first visits
14 the environment, he or she is prompted to enter an e-mail address). If the e-mail
15 address does not match one of those selected for the group, access to the environment
16 would be denied.

17 Turning to FIG. 14B, prospective group members can also be "invited" to join
18 the group. The user creating the environment can specify one or more e-mail
19 addresses to which an invitation will be sent. The invitation can be a simple text
20 message, or it could be a more sophisticated video or audio message. An expiration
21 date can also be associated with the invitation, such that responses to the invitation
22 received after the date will not be accepted. Software resident in web server 1201
23 (FIG. 12) receives responses to the invitations and adds members to the appropriate
24 group or drops them if the expiration date has passed or the prospective group
25 member declines participation. Prospective members can join the group by sending
26 a reply with a certain word in the message (e.g., "OK" or "I join"); by clicking on a
27 button in an e-mail message; or by visiting a web site identified in the invitation.

28 Turning to FIG. 14C, group members can also be solicited by creating an
29 advertisement directed primarily at potential group members that are unknown. The
30 advertisement could include, for example, a banner ad comprising text, video, and/or
31 audio clips. The graphic should conform to the size designated for the ad on the web
32 page. The ad could be posted on a web site by uploading the graphic through a web
33 interface and, optionally providing a URL on the screen of FIG. 14C to link to if the

1 advertisement is clicked. Software on the group page can render advertisements on
2 a page either (a) every time the page is displayed, (b) in rotation with other ads; or
3 (c) when characteristics of the user match criteria specified for the ad.

4 The advertisement can include an expiration date after which responses would
5 no longer be accepted. Advertisements could range from the very specific (e.g., an
6 advertisement posted on a school's home page advertising participation in Joe's
7 research project on drug use at the school) to more general (e.g., an advertisement
8 that says "we're looking for minority contractors looking to establish a long-term
9 relationship with us" that is posted on web sites that cater to the construction
10 industry.

11 A qualification option can also be provided to screen prospective group
12 members. For example, if an advertisement seeks minority contractors to participate
13 on a particular construction project, selecting the "qualify" option would screen
14 responses by routing them to the user that created the group (or some other authority)
15 before the member is added to the group. Those responding to the advertisement
16 could be notified that they did not pass the qualifications for membership in the
17 group, or that further information is required (e.g., documents evidencing
18 qualifications) before participation in the group will be permitted. Alternatively, an
19 automatic qualification process can be provided to allow a prospective member to
20 join if the person fills in certain information on the response (e.g., e-mail address,
21 birthdate that meets certain criteria, or the like).

22 As shown in FIG. 15, a banner ad displayed on a web site invites minority
23 contractors to join a group that bids on information technology contracts. Those
24 interested in the advertisement click a button, which leads them to another site (not
25 shown) requiring that they provide certain information (qualification information,
26 name, age, company registration information, etc.) This information is then
27 forwarded to web server 1201 which either pre-screens the information according to
28 pre-established criteria, or notifies the user creating the group that a prospective
29 member has requested access to the group. In the latter case, the user could screen
30 the applicant and grant access to the group.

31 FIG. 16 shows one possible user interface for selecting communication tools
32 to be made available to group members. This screen can be presented to the user
33 creating the environment after the group has been identified and its members

1 selected. It is contemplated that a variety of communication tools can be provided,
2 including a bulletin board service; advertisements; white pages (e.g., a listing of
3 members, their e-mail addresses, telephone numbers, and the like); yellow pages
4 (e.g., a listing of services or companies represented by group members, with
5 promotional and contact information); document security (e.g., shared access secure
6 document storage services); anonymous e-mail (described above with respect to the
7 first embodiment); threaded dialogs; a group newsletter creation tool;
8 videoconferencing; and even other user-provided applications that can be specified
9 by name and location (e.g., URL). Details of these services are provided below.

10 According to various preferred embodiments, dynamic collaborative
11 environments are designed to integrate tools from multiple sources provided that they
12 are web-accessible (i.e., they operate according to Internet Protocol and/or HTML-
13 type standards). The categories listed above provide a reasonable taxonomy of the
14 tools necessary for collaboration, but this list can be extended to include virtually
15 every class of software such as computer-assisted design, engineering and financial
16 analysis tools and models, office applications (such as word processing and
17 spreadsheets), access to public or proprietary databases, multimedia processing and
18 editing tools, and geographic information systems. The following describes some
19 of the communication tools that can be provided:

20 Bulletin boards. A bulletin board (see, e.g., FIG. 2) lists notices posted by
21 group members, which may be offers to buy or sell, but need not be limited to such
22 offers. Many types of bulletin board services are of course conventional and no
23 further discussion is necessary in order to implement one of these services.
24 Nevertheless, in one embodiment the following data items (attributes) can be
25 provided for each notice appearing on the bulletin board: an item number, a title, the
26 date posted, and one or more special attributes defined by the user. The attributes
27 may include a field to indicate whether a listing is a "buy" or "sell" offer. The board
28 can be provided with an integrated sorting capability. By clicking on the heading
29 of each column, the user can sort the entries in, alternately, ascending or descending
30 order. Thus, it is possible to organize the records from oldest to newest or newest to
31 oldest, or to separate buy and sell offers. To limit the values on a board, a search
32 capability can also be provided, such that only those entries that meet the search
33 criteria are displayed.

1 Advertisements. In a typical environment of a dynamically created network
2 there are a number of fixed places for advertisements – the top of a page for a banner,
3 the bottom of a page for a banner, and space on the side for small ads. The creator
4 of the environment may choose to use none, any, or all of these spaces for
5 advertisements. Once a space is designated for advertising, group members may
6 place adds by completing a template that provides payment information (if required),
7 the text for the ad (any standard image format), and a link to be executed if the ad is
8 clicked by someone viewing the ad.

9 Each user is responsible for providing functionality behind the link. The ad
10 may be displayed persistently (every time a page is displayed), in rotation with other
11 ads for the same place, or may be triggered on the basis of user characteristics
12 including purchasing history. Revenue can be collected for placement (fixed price
13 regardless of how many times an ad is displayed), per time that the ad is displayed,
14 or per click on the ad. The virtual private network provides the front-end to facilitate
15 online placement of the ad. Display can be done by linking pages to standard ad
16 display code, available off the shelf from several sources. This code provides for
17 rotation of the ads. Software for customization (i.e. choosing the ad based on user
18 characteristics) is available commercially from several sources.

19 White pages. White pages provide a comprehensive listing or directory of
20 members with information about them and information regarding how to contact
21 them. Various types of commercially available software can be used to manage such
22 directories, and it is elementary to code typical directories that have fixed contents
23 for each member.

24 A web-accessible directory can be used in accordance with various
25 embodiments of the invention. One type of directory that can be provided differs
26 from directories having fixed structures. The key differences are as follows:

27 (a) User control over information. Users enter and maintain their own
28 information directly, rather than through a central organization. This provides more
29 immediate update of data and reduces transcription errors. It makes it simple, for
30 example, for people to change their phone number when they are temporarily
31 working at another location.

32 (b) Multiple points for quality control. The data regarding each user can be
33 displayed to the user periodically (e.g.30, 60, and 90 days), and the user prompted to

1 update and verify the data. A feedback capability can be provided for members of
2 a group to report errors they find. Email addresses can be "pinged" periodically to
3 determine if they still exist. In addition, server management staff can periodically
4 review accounts that have had recent activity.

5 (c) Object structure. A directory entry consists of a collection of data
6 elements. These elements include such things as name for addressing (Dr. John D.
7 Smith), sort name (Smith, John D), or primary work telephone (800-555-1212).
8 Traditional mail systems have a fixed number of rigidly formatted elements. In one
9 embodiment, a more flexible approach can be used in that individuals identify which
10 elements they wish to add to the collection comprising their directory entry. For
11 example, a person can add 3, 4, 5 or more telephone numbers attaching a note to each
12 explaining its use (e.g. "for emergencies after 8PM").

13 (d) Direct link to communications tools. Where a directory refers to a contact
14 method (e.g. a telephone number), the method can be invoked directly from an entry
15 if the necessary software is available. For example, phone number can be dialed,
16 email messages initiated, or a word processing session initiated with letter and
17 envelope templates, preloaded with address information.

18 (e) Descriptive information. In addition to contact information, each directory
19 can contain information describing the entry (individual or business). The
20 description can be different in each group or it can be the same. The descriptive is
21 free form, with the exception that the user may drop in terms from a group-specific
22 lexicon. This lexicon can include terms specific to the industry (e.g. "fuel system")
23 for the automotive industry, or preferred forms of standard terms (e.g. "California"
24 rather than "CA", "Ca", or "Calif."). Standardization of terms in this way makes
25 search the directory more reliable.

26 Yellow pages. Conventional "yellow pages" products provide a one level
27 classification of directory entries designed to facilitate identification of and access
28 to an individual or organization with specific interests and capabilities. Within
29 industries, and particularly online, multi-level hierarchical directories are common,
30 with the multiple levels providing more precise classification. There are numerous
31 commercial products for maintaining online yellow page type classification systems.

32 Any web-accessible directory can be connected to a DVPN group. A
33 preferred method offered with the system integrates the classification system with the

1 descriptive field in a directory entry. Every time a standard term pertaining to a
2 classification is pulled from the lexicon, the entry is added to that classification in the
3 hierarchical sort. In addition to hierarchical access, this correspondence between the
4 traditional hierarchical sort and the free-form description with standardized terms
5 makes it possible to access records via search rather than browsing the hierarchy.
6 Searching makes it possible to identify an organization with multiple capabilities
7 (e.g. "brake repair" and "frame straightening"). This search capability is much like
8 a general web-search using a tool like AltaVista's or Inktomi's search engine and can
9 use the same search engine, but differs in that material being search is in a precisely
10 defined domain (group members), the information being searched is limited and
11 highly quality controlled (i.e. group directory entries), and has a precision rooted in
12 a precise vocabulary (the lexicon used in preparing the description).

13 Document repository. Any commercial web-enabled document repository
14 can be integrated into a group. Examples are Documentum and PC DOCs. An
15 improved version offered specifically with the DVPN package was described above.

16 Document security. Within the document repository various tools can be
17 provided to protect the security of documents. These include (1) limiting access to
18 a document to certain people or groups; (2) only displaying the directory entry for
19 documents to people who can access it; (3) password protection; (4) encryption; (5)
20 secure archive in read only mode on a third-party machine; (6) time-limited access
21 and (7) a secure hash calculation.

22 All of the above are conventional except for time-limited access and the
23 secure hash calculation. Software for limiting access to a document to a certain
24 period is available from Intertrust, among others. A secure hash is a number that is
25 characteristic of the document calculated according to a precisely defined
26 mathematical algorithm. There are several secure hash algorithms, and implementers
27 can develop their own. They are "trap door" in nature. That is, the calculation can
28 be performed with reasonable effort, but the inverse of the function is
29 computationally intractable. The classic example of a trap door function is
30 multiplication of very large prime number (on the scale of hundreds of digits). The
31 product can be calculated with relative ease, but factoring the product (the inverse
32 function) is very time consuming, making it effectively impossible with generally
33 available hardware. This method is used in public key encryption, but can be applied

1 equally well in secure hash, though other trap door functions are preferred, in
2 particular, the one specified by the U.S. Department of Commerce as FIPS standard
3 180. Code to implement this standard can be developed from published algorithms.

4 Anonymous e-mail (described above with respect to the first embodiment);
5 Threaded dialogs. Threaded dialogs are a collection of messages addressing
6 a specific topic, added serially, not in real time. They are threaded in the sense that
7 new topics can branch off from a single topic, and topics can merge. According to
8 one embodiment, threaded dialogs differ from conventional news group functionality
9 in that (1) users can initiate new topics; (2) users can post a message to one topic,
10 then indicate that the message pertains to other topic as well; (3) browsers reading a
11 message may continue down the original thread or one of the alternates if other topics
12 are suggested.

13 Group newsletter creation tool. A newsletter creation tool can be used to link
14 columns provided by multiple users (and maintained as separate web documents) into
15 a whole through an integrating outline maintained by an "editor". The purpose of
16 the tool is to provide the look and feel of an attractive single document to a disparate
17 collection. To create the newsletter the editor generates an outline identifying an
18 author for each component and a layout. Art for the first page can be provided.
19 Through messaging, the authors are provided a link to upload their content. Content
20 is templated to include a title, date, a by line, one or more graphic elements, a
21 summary for the index, and text. The editor may allow documents to go directly to
22 "publication" or require impose a review and editing step.

23 Chat groups. Real time chat room software is widely available from many
24 sources including freeware and shareware.

25 Audio and videoconferencing. Commercially available tools for web-based
26 audio and video conferencing can be included in the group functionality. Examples
27 are Net Meeting and Picture Tel software.

28 FIG. 17 shows one possible user interface for selecting research tools to be
29 made available to group members. As shown in FIG. 17, various tools such as a
30 mortgage calculator, LEXIS/NEXIS access, news services, Valueline, and other
31 research tools can be provided by checking the appropriate box on the display. All
32 of these research tools are conventional and commercially available (via web-based
33 links and the like).

1 FIG. 18 shows one possible user interface for selecting transaction engines
2 to be made available to group members. As shown in FIG. 18, many different types
3 of transaction engines can be provided to group members, including electronic data
4 interchange (EDI) ordering; online catalog ordering; various types of auctions; sealed
5 bids; bid and proposal tools; two-party negotiated contracts; brain writing (moderated
6 online discussion) and online Delphi (collaborative estimation of a numerical
7 parameter). The following describes various types of transaction engines in more
8 detail. Enhanced features (i.e., those that differ from conventional products) are
9 highlighted in gray text.

10 A. Order placement (online catalog) transaction engine

11 An order placement or online catalog engine allows the buyer to place an
12 order for a quantity of items at a stated fixed price, essentially ordering from an
13 online catalog. The catalog contains the description and specification of the
14 offerings. The catalog may be publicly accessible (Subtype 1a) or provided for a
15 specific customer (Subtype 1b). Prices are included in the catalog but may be
16 customer specific, may vary with quantity purchased, terms of delivery and
17 performance (e.g. cheaper if not required immediately). The catalog can represent
18 a single company's offering or an aggregate of the offerings from several companies.
19 The catalog can range from a sales-oriented web site designed for viewing by
20 customers, to a engine designed only accept orders sent via electronic data
21 interchange (EDI). Note that the catalog can be shopper oriented (i.e. designed to
22 sell) or a simple, machine-readable list of available items and prices. The following
23 describes in more detail steps that can be executed to create an online catalog:

24 1. Enter and maintain a framework for catalog

25 1.1. Enter / delete / edit categories. Categories are titles for groups of items, such
26 as "furniture" or "solvents"

27 1.2. Enter / delete / edit subcategories. Subcategories are categories within
28 categories, effectively establishing a hierarchy of products. Example:
29 furniture/dining room/tables.

30 1.3. Create groups of categories and subcategories (e.g. "see also..."). The
31 grouping allows a person browsing items to be referred to another category
32 that may contains items of interest. For example, someone may reach the
33 furniture/dining room/tables and then be referred to

- 1 furniture/office/conference room tables where other suitable tables may be
2 listed, or to furniture/dining room/chairs to buy chairs that make the table.
3 This cross-referencing transforms the hierarchical arrangement of
4 categories into a web.
- 5 2. Enter / edit / delete items in catalog by entering and updating the information
6 listed below. The system allows users to enter this information and provides
7 basic quality assurance.
- 8 2.1. Catalog item number
9 2.2. Supplier part number(s)
10 2.3. Name of item
11 2.4. Description
12 2.5. Photos and drawings
13 2.6. Specifications (depends on item type). Different items have different
14 specifications. For example, a computer printer can have color vs. black
15 and white, dots per inch resolution, paper size, etc. In contrast to a fixed,
16 hard coded catalog, the specification section of the general purpose
17 catalog engine the user prepares the specification section by selecting
18 parameters from a list and then specifying a value for that parameter.
19 The parameter list contains values such as length, width, height, voltage,
20 color, resolution etc. It is can be extended by the manager of the auction
21 environment. A lister selects a necessary parameter (e.g. length, then
22 enter the value, such as 14"). The specification section is a concatenation
23 of individual specifications.
- 24 2.7. First available date
25 2.8. Last available date
26 2.9. Category (categories) into which the item fits
27 2.10. Alternate suggestion(s) if product not available
28 2.11. Related and associated products (e.g. printer supplies for a printer or other
29 household items with the same pattern.
30 2.12. Additional information at the option of the individual or organization
31 listing the item.
- 32 3. Enter / update pricing information
33 3.1. Simple price. The fixed prices is per item or per unit. The price must

- 1 specify the
- 2 3.2. Pricing algorithm -- link to code for pricing algorithm
- 3 4. Take Orders
- 4 There are two variants: 4a: manual purchase in which a person browses a catalog
- 5 and selects and item for purchase and 4b: automated order in which a purchase
- 6 is initiated by an electronic message.
- 7 Variant 4a: Manual Purchase
- 8 4.1. Potential buyers access the catalog by drilling down through the category
- 9 / subcategory tree or
- 10 4.2. Buyers search fields in catalog to identify the appropriate item. The search
- 11 may examine the title, description, or any of the specification fields.
- 12 4.3. Display general information for item(s) meeting specifications
- 13 4.4. Allow user to modify search or to select specific item if the items displayed
- 14 to do not meet his requirements
- 15 4.5. Display detailed information for selected item
- 16 4.6. Display the fixed price or calculate price if price is based on an algorithm.
- 17 The pricing algorithm may include parameter such as characteristics or
- 18 affiliation of the users (e.g. affiliated with a pre-negotiated discount
- 19 program) , delivery date and mode, and quantity.
- 20 4.7. Offer the option to purchase or search again if they choose not to purchase.
- 21 4.8. If the buyer opts to proceed with the purchase, then check the availability of
- 22 the item by linking to the seller's inventory system
- 23 4.8.1. If the item is available then execute an 'add to basket'. That is, place
- 24 it on a list of items designated for purchase.
- 25 4.8.2. If the item is not available, then execute the contingent response:
- 26 4.8.2.1. Offer delivery at predicted date
- 27 4.8.2.2. Terminate the sale, but offer to deliver or notify when next the
- 28 item is next available.
- 29 4.8.2.3. Suggest alternate items
- 30 4.8.2.4. Report 'sorry' and abort transaction
- 31 4.9. Offer option to purchase additional options
- 32 4.9.1. If offer is accepted, execute from step 4.1
- 33 4.9.2. If offer is not accepted, proceed with step 4.10

- 1 4.10. Conclude the transaction
 2 4.10.1. Collect shipping information, offer options
 3 4.10.2. Collect payment information
 4 4.10.3. Validate payment
 5 4.10.4. Summarize order
 6 4.10.5. Obtain final authorization
 7 4.10.6. Generate receipt

8 Variant 4b: automated order, done using an EDI (electronic data interchange)
 9 message

10 4.1 Accept requests for item

11 4.2 Return price and confirmation of availability

12 Note that users may conduct transactions without employing EDI. It is
 13 possible, however, for members to agree on a transaction EDI format either by
 14 completing a template within the system or selecting a pre-established EDI format
 15 from a library. This library can include formats developed by recognized standards
 16 organizations (e.g. UNEDIFACT or ANSI) or formats developed specifically for an
 17 industry or a trading environment. Once there is agreement on a format, transactions
 18 can be initiated, concluded, and confirmed through the exchange of appropriate EDI
 19 messages. As many commercial ordering, accounts payable, accounts receivable and
 20 enterprise resource planning systems have an EDI interface the collaborative
 21 environment should have the capability to forward the message to the order
 22 fulfillment system.

23 B. English Auction Transaction Engine

24 In an English Auction, a single item is offered for sale to many buyers. The
 25 auction can be open or limited to pre-qualified bidders. The buyers offer bids in turn,
 26 each succeeding all prior bids. The highest bid received at any point in the auction
 27 is visible to all buyers. The identity of the highest bidder may or may not be visible
 28 to traders. Buyers may increase their bids in response to this information. Award
 29 is to the highest bidder at the end of trading. The end of trading is reached when
 30 there are no higher bids during an interval that may be formally defined or
 31 determined by the manager of the auction at the time of execution.

32 There are two models for the access to the transactions. In the first model,
 33 all buyers and sellers are members of the group. In the second model, all sellers are

1 members of the group, but buyers can include members and non-members. If non-
2 members are allowed to buy, the creator the transaction must enter a new URL for
3 buyers. This is a sub-URL of the main group URL. A registration process may be
4 established for the buyer URL.

5 In live auctions (as opposed to online) all traders are connected at the same
6 time, and the duration of the auction is brief – typically only a few minutes. In online
7 trading, it is not necessary for all of the bidders to be present (i.e. connected at the
8 same time). To distinguish between these two options they are designated (a)
9 concurrent (everyone bidding at the same time) and (b) batch (not everyone
10 connected simultaneously). The manager of the auction can set the minimum bid
11 and the minimum increment.

12 1. The first step in conducting an auction is to collect information on the items being
13 offered for sale. This is done online. The information collected includes:

14 1.1. Identity of seller. Note that the business rules of the auction may require
15 advance registration of sellers to verify their identity.

16 1.2. Descriptions, optionally including attachments and photographs, independent
17 certifications or appraisals, and anything else in digital form necessary or
18 useful in determining the value of the item.

19 1.3. Reserve price

20 1.4. Minimum increment

21 1.5. Time offered for sale

22 1.6. Time bidding is scheduled to end

23 1.7. Verify the seller's consent to the rules of the auction house regarding
24 delivery, payment, responsibility for non payment, etc.

25 2. If the business rule of the auction house is to require payment up front, collect
26 payment either by:

27 2.1. Debiting a deposit account

28 2.2. Charging to account for billing

29 2.3. Collecting online payment such as through a credit card.

30 3. Post information about auction, including:

31 3.1. Description of items to be auction

32 3.2. Auctions rules:

33 3.2.1. Qualification process for bidders

- 1 3.2.2. Time of bidding
- 2 3.2.3. Criterion for ending bidding – time between bids
- 3 3.2.4. Legal statement – responsibilities of buyer and seller, limitation of
- 4 liability
- 5 4. Execute qualification process (optional)
- 6 4.1. Admit bidders who are qualified based on past participation
- 7 4.2. Provide fill-in-the blank qualification form new bidders
- 8 4.3. Collect information
- 9 4.4. Conduct automated review or manual review
- 10 4.5. Inform prospective bidder of qualification or not
- 11 Variant (a): concurrent auction
- 12 5. Conduct Auction
- 13 5.1. Fifteen minutes prior to appointed time for auction, display “Welcome”
- 14 screen with space for qualified bidder to enter an alias or handle to be used
- 15 in the auction. Screen should have a description of the object. Show time
- 16 until auction starts. Auto refresh at 15 second intervals.
- 17 5.2. At appointed time, display the main auction page with the following
- 18 information:
- 19 5.2.1. Description / picture of item for auction stored in a separate, static
- 20 frame of the PC so that it does not need to be downloaded each cycle.
- 21 5.2.2. Current bid (initially the reserve price)
- 22 5.2.3. Suggested next bid (e.g. current + 3 * increment)
- 23 5.2.4. Button to accept suggested next bid
- 24 5.2.5. Field to enter bid higher than suggested next
- 25 5.2.6. Handle of the highest bidder
- 26 5.3. Refresh main auction page at 15 second intervals
- 27 5.4. Collect bids, either
- 28 5.4.1. Notice that the suggested bid was accepted
- 29 5.4.2. Bid higher than accepted bid
- 30 5.4.3. If new bid is lower than current highest, discard
- 31 5.4.4. If higher than current highest then
- 32 5.4.4.1. Log identity of highest bidder
- 33 5.4.4.2. Update highest bid

- 1 5.4.4.3. Update next suggested bid
- 2 6. If nobody accepts the suggested bid, then
- 3 6.1. Reduce suggested next bid
- 4 6.2. If accepted, resume normal sequence
- 5 6.3. If not accepted, reduce suggested next bid
- 6 6.4. If accepted, resume normal sequence
- 7 6.5. If not, begin close
- 8 6.6. "Going once ...", if response, resume normal sequence, else
- 9 6.7. "Going twice ..." if response, resume normal sequence, else
- 10 6.8. Done. Display closing screen
- 11 7. Settle with winning bidder, two models
- 12 7.1. Connect buyer to seller for direct settlement
- 13 7.2. Collect money from buyer, deduct fee, convey amount to seller
- 14 Variant (b): batch (i.e. time limited) auction
- 15 Conventional on-line batch (time limited) auctions are common. E-bay is
- 16 the most prominent example. This process description continues from step 4 of
- 17 the English auction description as the startup of the concurrent and batch auctions
- 18 are the same.
- 19 5. Conduct auction: Until closing time for an item:
- 20 5.1. On entry to system display the following for the potential buyer:
- 21 5.1.1. Latest listing
- 22 5.1.2. Categories
- 23 5.1.3. Search screen
- 24 5.2. On selection of categories:
- 25 5.2.1. Execute dill down
- 26 5.2.2. Retrieve count of items that meet criteria
- 27 5.2.3. If more count is less than 25 (or other small number (n)
- 28 consistent with the layout of the screen) retrieve all items that meet
- 29 criterion
- 30 5.2.4. If count is more than n, retrieve n auctions with nearest
- 31 expiration time
- 32 5.2.5. Display link list to all items in list, sort order should be
- 33 auction with nearest deadline to most distant

- 1 5.2.5.1. Item name
- 2 5.2.5.2. Time till end of auction
- 3 5.2.5.3. Highest current bid
- 4 5.2.6. On user selection of the item, display same information as above plus
- 5 5.2.6.1. Description
- 6 5.2.6.2. Photo (if any)
- 7 5.2.6.3. Attachments (if any)
- 8 5.2.7. If count is more than n, display further drill-down options as
- 9 well as item information above
- 10 5.3. Accept new bid through the display screen
- 11 5.3.1. Log bids in order, reject if bid is not higher than last high bid by
- 12 increment.
- 13 5.3.2. If bid is rejected, tell bidder that their bid is not sufficient
- 14 5.3.3. Update database recording highest bid, bidder, time of bid
- 15 5.3.4. Display screen to user to confirm that their bid is the highest
- 16 6. When the time limit is reached, determine if a new bid has been received in the
- 17 last 3 minutes (or other short time period). If so, extent the bidding time by 3
- 18 minutes (or other short time period) and execute step 5 with a new closing time.
- 19 7. When the time limit is reached, including all extensions under step 6, then
- 20 7.1. Email message to highest bidder that they won
- 21 7.2. Add transaction to completed deals
- 22 7.3. Update splash and add screens
- 23 7.4. Settle with winning bidder-- two models:
- 24 7.4.1. Connect buyer to seller for direct settlement
- 25 7.4.2. Collect money from buyer, deduct fee, convey amount to seller

26 C. Dutch Auction Transaction Engine

27 A Dutch auction, like a standard auction, involves the sale of a single item or

28 batch with fixed specifications. There is one seller, and many potential buyers. The

29 seller sets the prices, ideally higher than any buyer's maximum bid price. The

30 offered price is reduced by a fixed increment at fixed intervals until a buyer accepts

31 the price. The purchase goes to the first buyer in to accept the price. In the physical

32 world (as opposed to the online world), Dutch auctions are rarely if ever run

33 concurrently. In a live trading room, it could be difficult to determine which buyers

- 1 was first to commit to a price when several are willing to pay the same amount. The
2 Dutch auction is relatively simple to implement in an electronic environment. There
3 are, at present, no online Dutch Auctions of which the inventors are aware.
- 4 1. Enter and maintain a framework for catalog
 - 5 1.1. Enter / delete / edit categories. Categories are titles for groups of items, such
6 as "furniture" or "solvents"
 - 7 1.2. Enter / delete / edit subcategories. Subcategories are categories within
8 categories, effectively establishing a hierarchy of products. Example:
9 furniture/dining room/tables.
 - 10 1.3. Create groups of categories and subcategories (e.g. see also....). The
11 grouping allows a person browsing items to be referred to another category
12 that may contain items of interest. For example, someone may reach the
13 furniture/dining room/tables and then be referred to
14 furniture/office/conference room tables where other suitable tables may be
15 listed, or to furniture/dining room/chairs to buy chairs that make the table.
16 This cross referencing makes transforms the hierarchical arrangement of
17 categories into a web.
 - 18 2. Execute qualification process (optional)
 - 19 2.1. Admit bidders who are qualified based on past participation
 - 20 2.2. Provide fill-in-the blank qualification form new bidders
 - 21 2.3. Collect information
 - 22 2.4. Conduct automated review or manual review
 - 23 2.5. Inform prospective bidder of qualification or not
 - 24 3. Collect information on items to be auctioned and owners, including
 - 25 3.1. Identity of seller
 - 26 3.2. Descriptions, optionally including attachments and photographs, independent
27 certifications or appraisals, or other information necessary to establish the
28 value of the item
 - 29 3.3. Categorization
 - 30 3.4. Starting price
 - 31 3.5. Increment, Interval for reduction
 - 32 3.6. Minimum price
 - 33 3.7. Obtain consent to rules (possibly as part of registration/qualification process)

- 1 3.8. Collect to conduct auction if item is
- 2 3.9. Calculate time to take item off auction by determining the number of steps
- 3 (intervals) necessary to reduce price from the starting price to the
- 4 minimum
- 5 3.10. Record all of the above information in the Dutch auction database
- 6 4. Cull expired options
- 7 4.1. Search database periodically for items where current time is later than time
- 8 to take item off auction (2.9)
- 9 4.2. Inform owner that item was not sold
- 10 4.3. Delete entry from database
- 11 4.4. Prompt for revised terms start of another auction, create new entry if user
- 12 takes option
- 13 5. When the buyer enters the system display a list of high level categories, a prompt
- 14 for search criteria, and/or a link to a search page. Allow user to drill down
- 15 through categories or enter search parameters.
- 16 5.1. Retrieve count of items that meet criteria
- 17 5.2. If more count is less than 25 (or other small number (n) consistent with the
- 18 layout of the screen) retrieve all items that meet criterion
- 19 5.3. If count is more than n, retrieve n auctions with nearest expiration time
- 20 5.4. Display link list to all items in list, sort order should be auction with nearest
- 21 deadline to most distant
- 22 5.4.1. Item name
- 23 5.4.2. Time till end of auction
- 24 5.4.3. Current price:
- 25 5.4.3.1. Retrieve starting price (SP) and increment (IS)
- 26 5.4.3.2. Calculate number of intervals since start of auction (INT)
- 27 5.4.3.3. Determine price = $SP - (INT * \$)$
- 28 5.5. On click, display same information as above plus
- 29 5.6. Description
- 30 5.7. Photo (if any)
- 31 5.8. Attachments (if any)
- 32 5.9. The display screen should include a button that allows the buyer to purchase
- 33 the item at the selected price.

- 1 6. When the user clicks the "buy" button
- 2 6.1. Email message to highest bidder that they won
- 3 6.2. Add transaction to completed deals database
- 4 6.3. Settle with winning bidder-- two models:
- 5 6.3.1. Connect buyer to seller for direct settlement
- 6 6.3.2. Collect money from buyer, deduct fee if any for auction and
- 7 payment services, convey the remainder to seller.

8 D. Reverse English Auction Transaction Engine

9 In a reverse auction, there are multiple buyers to one seller. Prices come
 10 down rather than up. There are many variants of a reverse auction. The variant
 11 discussed here is a reverse English auction. Reverse auctions have been
 12 implemented on line in Open Markets.

13 The process for posting an item for bid and for qualifying bidders is the
 14 same as for other auctions. The difference here is that the buyer may optionally
 15 set a maximum price.

- 16 1. Accessing the list of items sought
- 17 Potential bidders access items sought by working through a hierarchy of
- 18 categories and subcategories or entering search criteria, as for other auctions. A
- 19 list of items within the category/subcategory and/or meeting the search criteria
- 20 is displayed. The user may then
- 21 1.1. Terminate the session on finding no suitable items
- 22 1.2. Revise the search criteria
- 23 1.3. Select an item on which to bid
- 24 2. If the user selects an item on which that may wish to bid, detailed information
- 25 about the items is displayed. This item may include the following information:
- 26 2.1. Name
- 27 2.2. Seller
- 28 2.3. Description
- 29 2.4. Detailed specifications for items
- 30 2.5. Delivery requirements
- 31 2.6. Proposed terms
- 32 2.7. Current low bid
- 33 3. If the user determines that they should bid, he accesses the bid entry screen from

- 1 the detailed description in Step 2 above. Making a bid consists of entering the
2 following information:
- 3 3.1. New, lower bid
4 3.2. Comments pertaining to any special terms, features, or conditions
5 3.3. Attachments containing relevant additional information and any
6 certifications required by the buyer
- 7 4. On receipt of bid, there are two options – either all bids are accepted, or bids are
8 accepted only after review of information by the buyer.
- 9 4.1. Case 1: all bids are accepted
- 10 4.1.1. New bid is checked to determine if it is lower than prior bid
11 4.1.2. If so, then
- 12 4.1.2.1. bidder is notified that their bid is currently the lowest
13 4.1.2.2. seller is notified of new low bid
14 4.1.2.3. bid database is updated
- 15 4.1.3. If not, then
- 16 4.1.3.1. Bidder is notified that their bid is not the lowest
17 4.1.3.2. Bid screen is displayed so that bidder may lower bid
- 18 4.2. Case 2: bids are accepted after review by buyer
- 19 4.2.1. Buyer is notified of bid via email or online message
20 4.2.2. Buyer accesses complete information on the proposed bid through the
21 system
22 4.2.3. Buyer select accept bid or reject bid.
23 4.2.4. If bid is accepted, then
- 24 4.2.4.1. Bidder is notified that their bid is currently the lowest
25 4.2.4.2. Bid database is updated
- 26 4.2.5. If bid is not accepted, then
- 27 4.2.5.1. Buyer enters reason for not accepting bid
28 4.2.5.2. Bidder is informed that bid is rejected with reason stated
29 above
30 4.2.5.3. Bidder may access the bid screen to revise offer
- 31 5. When time period has expired and there have been no bids within a short
32 specified interval, then
- 33 5.1. If at least one bid less than the maximum has been received, then:

- 1 5.1.1. Notify low bidder that their offer was successful
- 2 5.1.2. Add transaction to completed deals database
- 3 5.1.3. Settle with winning bidder-- two models:
- 4 5.1.3.1. Connect or introduce buyer to seller for direct settlement
- 5 5.1.3.2. Collect money from buyer, deduct fee if any for auction and
- 6 payment services, and convey the remainder to seller.
- 7 5.2. If no bid less than the maximum has been received, the
- 8 5.2.1. Notify buyer
- 9 5.2.2. Allow buyer to revise bid criteria

10 E. Sealed Bid Transaction Engine

11 In a sealed bid system, the buyer publishes or distributes detailed, fixed
 12 specification to a number of potential bidders (who may or may not be
 13 prequalified). Bidders submit binding bids by a specified deadline, in a specific
 14 format that allows ready comparison. The competitive bidding process is
 15 distinguished from the bid and proposal process by the complexity of the
 16 specifications and the bids. In a simple competitive bid, competition among the
 17 bidders is along one or two readily quantified dimensions (always including price)
 18 and there is little or no room for variation in the form or specifications of the
 19 offering. Comparison of the bids is elementary.

20 The process for posting an item for bid and for qualifying bidders is the
 21 same as for other transactions as is the method to identify items on which to bid
 22 either using the hierarchy of categories and subcategories or a search engine.

- 23 1. If the user selects an item on which he may wish to bid, detailed information
- 24 about the items is displayed. This item may include the following information:
- 25 1.1. Name
- 26 1.2. Seller
- 27 1.3. Description
- 28 1.4. Detailed specifications for items including all information necessary to
- 29 prepare a bid
- 30 1.5. Bid instruction including specification for any documentation the buyer may
- 31 required with a bid (e.g. proof of bonding or license)
- 32 1.6. Notice of any fees for bid registration
- 33 1.7. Delivery requirements

- 1 1.8. Proposed terms
- 2 2. After review of the bid requirements, the user may choose not to bid or may enter
- 3 a bid. The process for entering a bid consists of preparing a bid package,
- 4 including the price offered and any necessary supporting documentation. This
- 5 is done by completing an online form, with provision for attachments. The bid
- 6 is submitted through the system where it goes into a database of bids that are not
- 7 opened to the closing time for the bidding process.
- 8 3. At the closing time, all bid packages are conveyed to the buyer.
- 9 3.1. If there are no bids, the buyer is offered the opportunity to revise the request
- 10 for bids.
- 11 3.2. If there are multiple bids, the buyer reviews the bids and selects the lowest
- 12 priced qualifying bid. They buyer informs the seller and arranges payment
- 13 and delivery in accord with the terms stated in the bid package.

14 F. Order Matching Transaction Engine

15 In an order-matching system there are many potential buyers. Each posts

16 binding offer to buy (bid amount) or sell (asked amount). The process proceeds in

17 real time. The order matching system constantly compares bid and asked and, when

18 a match is found within a specified spread, the deal is concluded. No accepted offer

19 can be repudiated, but offers may be withdrawn before a deal is consummated. The

20 strike price is posted so that buyers and sellers can modify their offerings in real time.

21 The items traded are fungible so that price is the only decision. For the market to

22 operate efficiently the items traded must be tightly defined and the terms of sale must

23 be fixed and determined in advance. This is typically done by the operation or an

24 exchange, with the order-matching engine operating in the background. To insure

25 that the items traded are well defined, and the terms of sale are rigid example of an

26 order matching process in stock trading on an exchange.

27 Users of an order-matching engine are all potential buyers and seller. They

28 are qualified in advance using a process like that outlined by for auction with the

29 extension that deposit accounts are frequently required given the speed of

30 transactions in exchange environments.

- 31 1. Establish and maintain items to be traded. All functions in this category are
- 32 reserved to the manager of the exchange or a designee.

33 To add (i.e. "list" and idem), enter

- 1 1.1. Unique item number or symbol
- 2 1.2. Description of item (e.g. Sears Class A Common Stock)
- 3 1.3. Terms and conditions ownership (e.g. who can own) if any
- 4 1.4. Trading units (e.g. shares, blocks, etc.)
- 5 1.5. Additional information as required by the rules of the exchange
- 6 To delete (i.e. "delist" and item)
- 7 1.6. Select the item to be deleted
- 8 1.7. Confirm deletion
- 9 2. On entry to the system, potential buyers and sellers can review the price of the
- 10 last transaction of any item, either through a list or a search by item name or
- 11 symbol. The current highest asked and lowest bid price are also shown.
- 12 3. An offer to sell is posted by entering the following information:
- 13 3.1. Item number or symbol
- 14 3.2. Quantity offered
- 15 3.3. Proposed price ("asked")
- 16 3.4. Seller
- 17 3.5. Offers may be revise at any time prior to consummation of a deal
- 18 4. An offer to buy is posted by entering the following information
- 19 4.1. Item number or symbol
- 20 4.2. Quantity offered
- 21 4.3. Proposed price ("asked")
- 22 4.4. Buyer
- 23 4.5. Offers may be revised at any time prior to consummation of a deal
- 24 5. Offers to buy and sell are constantly reviewed by the software. When there is an
- 25 offer to buy and sell at a price within a preset difference. When prices match,
- 26 buyers and sellers are notified of the transaction, and the transaction is recorded.
- 27 The display of the last transaction price, the highest bid and the lowest asked
- 28 price is updated.
- 29 6. The transaction is conveyed to the backend accounting system of the exchange.

30 G. Bid and Proposal

- 31 The bid and proposal process is typically used for procurement of large or
- 32 complex products or services, in which cost is not the only factor. Cost must be
- 33 weighed against the buyer's assessment of the quality and suitability of an offering

1 and the ability of the bidder to deliver the product or perform the specified services.
2 The bid and proposal process is conducted between one buyer (possibly
3 representing a consortium) and many potential sellers, sometimes organized into
4 teams. The buyer issues specifications that may be general or highly specific, brief
5 or very lengthy. The specifications may be distributed freely or to a list of qualified
6 buyers.

7 With physical RFPs, the size and the associated cost of distribution make it
8 common practice to advertise the availability of the RFP first, sending copies only
9 to those that request it. Frequently, the requestors are required to supply information
10 to establish their qualifications to bid. While cost is not an issue in electronic
11 dissemination of RFPs, the model of advertising prior to distribution is still useful in
12 managing the qualification process. This is addressed as variant (a) in this
13 description. Variant (b) requires no prequalification.

14 In a competitive bid on fixed requirements (sealed bid or auction), there is
15 typically very little communication between buyer and seller between publication of
16 the request and submission of the bids. The requirements are comparatively simple,
17 clear, and unambiguous. In contrast, the bid and proposal process may involve
18 considerable communication between buyer and seller. The process may begin with
19 a bidders' conference to answer questions about the requirements. Additional
20 questions from bidders may be accepted, though not all need be answered.
21 Questions and answers may be made available to all bidders or the response may be
22 in private. This dialog is crucial for two reasons. First, it helps the bidders
23 understand the requirements and to be responsive in their bids. Second, it is not
24 unusual for the bidders' questions to identify some point of ambiguity, error, or
25 contradiction in the specifications, leading to a modification of the RFP. The
26 diverse perspectives of the bidders, and the close attention required on their part to
27 prepare a bid inherently provides an excellent review of the RFP.

28 The initial phase of the RFP process concludes with submission of the bids,
29 but this is far from the conclusion of the process. Commonly, questions arise from
30 the review of the proposals. These may relate to a specific submission or have
31 broader implications, leading to modification of the requirements. The list of
32 bidders can be culled to the best candidates. These are asked to answer questions
33 about their proposals and to provide additional and clarifying information.

1 The process described here is built around the document repository described.
2 elsewhere in this application. Through this process of refinement, the list of bidders
3 is narrowed to one or two with whom a contract is negotiated. The process of
4 negotiation is addressed as a separate transaction type (Negotiation Engine) as it may
5 be conducted without the bid and proposal process.

6 Variant (A): with pre-qualification

- 7 1. Software supports the user in creating a web site for the proposal process.
8 Initially this site manages the process for requesting the request for proposal
9 (RFP), qualifying bidders, and disseminating the RFP.
- 10 2. Supported by the system software, the bidder creates and RFP advertisement by
 - 11 2.1. entering a summary of the RFP.
 - 12 2.2. entering a summary of the information needed to qualify as a bidder or
 - 13 2.3. attaching a form (HTML web page or template for paper form) for entering
14 qualifying information
- 15 3. The RFP advertisement includes file transfer software for uploading qualifying
16 information to the repository.
- 17 4. Disseminate RFP advertising
 - 18 4.1. Post on public bulletin board or
 - 19 4.2. Disseminate via mail to selected users
- 20 5. When users access the system, issue them an encryption key and PIN to be used
21 for subsequent uploads and communications to verify their identity.
- 22 6. Receive requests for RFP in repository
 - 23 6.1. Prompt for key
 - 24 6.2. Encrypt submission
 - 25 6.3. Upload
 - 26 6.4. Generate receipt – should include an authentication number
- 27 7. Disseminate RFP to selected user, either:
 - 28 7.1. Attach to return Email or
 - 29 7.2. Post the RFP in a repository from which qualified prospective bidders may
30 download the file. If the repository model is used, provide notice of the
31 posting via email including any necessary PINs and codes to access the
32 repository
 - 33 7.3. When a prospective bidder downloads an RFP, issue an encryption key to be

- 1 used in submitting proposal
- 2 8. The RFP site also includes a page through which prospective bidders can submit
- 3 questions. Questions and answers are posted to the site.
- 4 9. Updates to the schedule and amendments to the RFP are posted to the site
- 5 10. All access to the site is recorded to verify that prospective bidders have received
- 6 critical information. Direct contact may be used when it is determined that a
- 7 bidder had not accesses the site since critical new information was posted.
- 8 11. Bidders prepare their proposal and then upload them to a repository for proposals
- 9 using software built into the proposal site.
- 10 11.1. Prompt for key
- 11 11.2. Encrypt submission
- 12 11.3. Upload
- 13 11.4. Generate secure hash number to prevent tampering with the
- 14 submission
- 15 11.5. Generate receipt including secure hash number and authentication
- 16 code
- 17 12. After initial proposals are received, the process moves into a phase commonly
- 18 termed the "best and final process" in which the proposals are reviewed, the list
- 19 narrowed, and the proposals refined.
- 20 12.1. Create separate secure environment (i.e. web site with repository) for
- 21 each respondent
- 22 12.2. Exchange materials through repository (described elsewhere in this
- 23 filing)
- 24 12.3. Records and receipt each access
- 25 12.4. Generate key for revised proposal
- 26 12.5. Receive proposal using process in 11
- 27 12.6. Repeat from step 11 as many times as necessary
- 28
- 29 The remainder of the process is completed as a negotiated deal, described below.
- 30 Variant B: no pre-qualification:
- 31 Proceed as above, beginning with Step 6 and not requiring a key for download of the
- 32 RFP.

1 H. Negotiation Deal Engine

2 An engine for negotiating a deal can be built around the capability of the
3 system to create a temporary virtual private network through the web. A temporary
4 network is created for the negotiation. Access to the network is limited to the parties
5 of the negotiation, their advisors and counsel, and, potentially, arbitrators and
6 regulators. The members of the negotiating environment have access to the complete
7 set of tools described in this filing including those for communications (email,
8 anonymous mail, online chat, threaded dialogs, and audio and video collaboration),
9 the library of standard contract instruments, the tools for document signature and
10 authentication, and the document repository. Using these tools in a secure
11 environment they can negotiate, close, and register a deal.

12 FIG. 19 shows one possible user interface for selecting participation engines
13 to be made available to group members. The term "participation engine" refers
14 generally to collaboration tools that provide features beyond merely communicating
15 among group members. Various services such as an on-line survey tool, a DELPHI
16 model tool; brain writing tool; and real-time polling can be provided.

17 A. Online Survey

18 In online polling or surveying, the person creating the poll uses and
19 automated tool (new to this application) to build simultaneously an online
20 questionnaire and a database to collect the results. The user builds the questionnaire
21 by entering a series of questions and an associated data collection widget for each.

22 The polling tool builds the database and the data entry screen. The data entry
23 screen consists of two columns. The left column is a series of questions. The right
24 column is the data entry tool appropriate to the question. Various data entry tools
25 can be provided to respond to the query, including such things as:

- 26 1. yes / no radio buttons
- 27 2. true / false radio buttons
- 28 3. slider with scale from 1-5, 1-10, etc.
- 29 4. fill-in-the-blank text box
- 30 5. numeric field
- 31 6. multiple check boxes (e.g. strongly disagree, disagree, agree, strongly
32 agree)

33 Other data entry types may be added.

1 As each question / data collection widget is added, the polling tool creates the
2 database. The database includes one record per data collection form. Creating the
3 database structure simply means adding one new field to each record definition for
4 each question. The type of data collection widget defines the format of the field, as
5 follows:

- 6 1. yes / no radio buttons: one character field, limited to "y" or "n"
- 7 2. true / false radio buttons: one character field, limited to "y" or "n"
- 8 3. slider: real number field, with appropriate range check
- 9 4. fill-in-the-blank text box: text box
- 10 5. numeric field: real number or integer
- 11 6. multiple check boxes: integer field with range check from 1 to number of
12 boxes

13 Every data entry screen provides a "save" and "cancel" button. Save writes to the
14 database. Cancel exits the entry screen without saving.

15 The survey, once composed as described above exists as a web page. This
16 page can be embedded in web applications. It can be made available on a site
17 available to the entire Internet, on an Intranet, or in a dynamically created
18 environment. Alternatively, it can be distributed via e-mail. When the form is
19 completed, the submit button transmits the value entered to the database that is
20 created at the time the form is generated. Access to the database is controlled by the
21 rules of the database system. It may be limited to the individual who creates the
22 survey form and database, but it may be accessible other users in the survey
23 developers organization, as determined by the database administrator. Distribution
24 of the result of the analysis is at the discretion and control of the individual managing
25 the survey. This manager may be the individual who creates the survey, but the
26 actual creator may be acting on behalf of the survey manager. Results may be kept
27 private, posted to the Internet, and intranet, or a collaborative environment,
28 distributed via e-mail within an organization, or, if the information is available, sent
29 via e-mail to the participants in the survey.

30 B. Online Delphi Engine

31 The online Delphi engine allows real-time collaboration in estimating or
32 predicting an outcome that can be expressed numerically. For example, the method
33 can be used to develop a consensus forecast of grain prices. The method has been

- 1 in used since the 1970s, but has not previously been adapted to online processes.
- 2 One possible method is as follows:
- 3 1. Establish the session
 - 4 1.1. Within an online community, the moderator of the session creates the brain
 - 5 writing session by entering the following information:
 - 6 1.1.1. Name of moderator
 - 7 1.1.2. Title of the session
 - 8 1.1.3. Description of the session
 - 9 1.1.4. Background reading as references or attachments
 - 10 1.1.5. Start date for the session
 - 11 1.1.6. Scheduled end for the session
 - 12 1.1.7. Access to the session:
 - 13 1.1.7.1. URL for access
 - 14 1.1.7.2. Open to all or invitees only for observation
 - 15 1.1.7.3. Open to all or invitees only for participation
 - 16 1.1.8. Payment information if required
 - 17 2. Optionally, the session may be advertised on line
 - 18 3. If the session is private, invitations with logon keys must be distributed via email,
 - 19 actual mail, or download.
 - 20 4. Optionally, the moderator may run on online applications and qualification
 - 21 process
 - 22 5. Prior to the start of the session, the moderator must describe precisely the value
 - 23 to be estimated. The definition must be completely unambiguous.
 - 24 6. Each participant connects at the start of the session. On connecting, they question
 - 25 is posed (e.g. "What will be the price of West Texas intermediate oil in
 - 26 December?")
 - 27 7. Each participant enters a number a brief (1 paragraph maximum) explanation of
 - 28 their reasoning.
 - 29 8. When the participant is done entering their estimate, they click "Done".
 - 30 9. Each participant's estimate and explanation is recorded.
 - 31 10. Each participant then sees the summary screen.

- 1 11. Estimates are arrayed graphically from top to bottom of the screen, from lowest
2 to highest. The value is stated as is the associated comment, but the source of
3 the comment is not revealed.
- 4 12. Participants can review the estimates and comments, send an anonymous message
5 to the author or any comment, or amend their answers.
- 6 13. The session terminates when the time expires, or when the moderator determines
7 that there it is no longer appropriate to continue. The operator may determine
8 this is based on declining participation or, if participation is high, the moderator
9 may extend the deadline.
- 10 14. Participants and observers may access the final display of estimates, again
11 arrayed from top to bottom, lowest to highest.

12 C. Brain Writing

13 Brain writing is a variant of a method for facilitated group discussion termed
14 brainstorming. The objective of brainstorming is to maintain the focus of the
15 discussion while encouraging creative input and recognizing the contributions of all
16 members of the group. It seeks to avoid problems with a few individuals dominating
17 the discussion, with junior staff deferring to senior staff, and with new ideas being
18 abandoned before than can be developed fully. Brain storming has been commonly
19 used since the late 1960s. Brain writing is a more intense method that relies on joint
20 writing rather than discussion. What is presented here is adaptation of that method
21 to an online environment. It is believed to be the first such adaptation.

- 22 1. Establish the session
- 23 1.1. Within an online community, the moderator of the session creates the brain
24 writing session by entering the following information:
- 25 1.1.1. Name of moderator
- 26 1.1.2. Title of the session
- 27 1.1.3. Description of the session
- 28 1.1.4. Background reading as references or attachments
- 29 1.1.5. Start date for the session
- 30 1.1.6. Scheduled end for the session
- 31 1.1.7. Access to the session:
- 32 1.1.7.1. URL for access
- 33 1.1.7.2. Open to all or invitees only for observation

- 1 1.1.7.3. Open to all or invitees only for participation
- 2 1.1.8. Payment information if required
- 3 2. Optionally, the session may be advertised on line
- 4 3. If the session is private, invitations with logon keys must be distributed via email,
5 actual mail, or download.
- 6 4. Optionally, the moderator may run on online applications and qualification
7 process
- 8 5. Prior to the start of the session, the moderator must list some number (typically
9 5-10) of questions or hypotheses to be explored. (e.g. " Our company should
10 create a spinoff to develop and commercialize the new breast cancer vaccine")
11 This may be done by the moderator alone, in consultation with the participants,
12 or with other outside the session.
- 13 6. Each question or hypothesis becomes a "Card".
- 14 7. Participants may enter the session any time after the start. A password may be
15 required if the session is not open.
- 16 8. On entry into the system, a user is given a card at random. The card consists of
17 the initial question or hypothesis plus all comments entered on the card by other
18 participants.
- 19 9. After reviewing the card, the participant may add his or her own comments to the
20 bottom. After entering comments, the participant clicks "Done" to return the
21 card to the pile.
- 22 10. When a participant returns a card to the pile, they received another card, chosen
23 at random (preferably) or selected by the user. This process continues until the
24 opt to exit. They may reenter at any time up to the conclusion of the session.
- 25 11. When a card is returned to the pile, it is become available for assignment to the
26 next participant. The card includes the additions of the most recent participant.
- 27 12. A participant may opt to return the card without addition if he or she has nothing
28 to add.
- 29 13. Participants may create new cards when new ideas come to mind. These are
30 treated in exactly the same way as original cards.
- 31 14. Observers may view any card but may not add to them.
- 32 15. The moderator may limit participation to a set number at any time so that there
33 is a sufficient number of cards to keep the participants fully occupied.

1 16. The session terminates when the time expires, or when the moderator determines.
2 that there it is no longer appropriate to continue. The operator can determine this
3 based on declining participation or, if participation is high, the moderator may
4 extend the deadline.

5 17. The raw cards are distributed at the conclusion to all participants. The moderator
6 or another individual is charged preparing a summary and arranging follow-up.

7 FIG. 22 shows one possible scheme for storing brain card writing data
8 elements. In accordance with one embodiment, each brain writing card comprises
9 a data structure including the following elements:

- 10 1. Brain writing session number: Serially assigned number to differentiate
11 brainwriting sessions. A session is the set of all cards pertaining to a
12 particular topic.
- 13 2. Card number: A Serially assigned sequence number
- 14 3. Initial Comment : The question or comment used to initiate the discussion
15 (e.g. "SAIC should purchase a company that produces Internet server
16 software")
- 17 4. Date and time card started
- 18 5. Date and time card closed
- 19 6. Comments: A collection (i.e. a set of unlimited length) containing the
20 comments added by participants in the brainwriting session.
- 21 7. Date of additional comment: Date and time that each additional comment
22 was added.
- 23 8. Commenter: Name or user ID of the person adding each additional
24 comment. Ideally, brainwriting should be anonymous to encourage open
25 dialog. Accordingly, this field may be omitted from an implementation.
26 Some organizations, however, may wish to track this information
27 without making it visible to users, or in some cases to attribute comments.

28 When the user has finished defining the group and specifying its functions,
29 environment generator 1201a (FIG. 12) creates an environment accessible to the
30 group members and including the functions specified during the environment
31 definition process. As shown in FIG. 20A, for example, a web page can be created
32 for the newly created environment, including those functions that were selected by
33 the user that created the group. All group members are notified of the existence and

1 location of the environment, and each group member can use the functions provided
2 in the environment to collaborate on a project or conduct business.

3 FIG. 20B shows what an environment might look like to a group member
4 after entering the environment. As shown in FIG. 20B, for example, a news banner
5 announces the latest news for the group. Additionally, specific communication tools,
6 research tools, transaction engines, and participation engines are made available to
7 group members, which can be executed by appropriate mouse clicks in accordance
8 with the inventive principles. According to various inventive principles, each tool
9 shown on the web page is accessible through a hyperlink to a web-based program that
10 performs predefined functions as set forth above. For example, clicking on "online
11 catalog" would link the group member to a web page that implements an online
12 ordering engine as described previously. Users can navigate through the various
13 tools using conventional web browser features (i.e., forward, backward, etc.). It may
14 be desirable to implement some or all of such software using server-side scripting or
15 other similar means consistent with the system configuration of FIG. 12.

16 FIG. 21 shows how environment generator 1201a can create multiple
17 environments including virtual private facilities, which can be implemented through
18 web pages that contain hyperlinks to functions available to members of each group
19 or environment. An environment definition software component 2106 implements
20 steps 1101 through 1103 of FIG. 11 in order to create one or more environments
21 2107. (In one embodiment, each group can also be provided with a copy of an
22 environment generator 2106 in order to create sub-groups that draw on the
23 applications and directory structure created for the group). As a user identifies group
24 members and selects functions to be provided for the environment in which the group
25 will collaborate, environment definition component 2106 stores information relating
26 to the selected members and functions in databases. Each environment can include
27 a web page (not shown in FIG. 21) and directories, tools and other applications
28 specific for each created group.

29 Based on user selections of the type illustrated in FIGS. 13 through 19,
30 environment generator 2106 creates an environment 2107 containing one or more
31 web pages with links to the selected tools. Environment generator 2106 retrieves
32 information from various information sources including a directory of
33 communication tools 2101 (e.g., including descriptions of tools and URL/IP

1 addresses of web applications to set up each communication tool); directory of
2 transaction engines 2102 (e.g., including descriptions of transaction engines and the
3 URL/IP addresses of web-based applications to set up each transaction engine);
4 directory of research tools 2103 (similar to above); list of global data objects 2104
5 (e.g., a dictionary of data elements from which the directory of each group can be
6 composed); and a directory of applications 2105 (e.g., a description of available
7 applications and URL/IP addresses of pages to set up access to applications).

1 **WE CLAIM:**

2 1. A method of negotiating a deal over a network of computers, the network
3 including at least one or more computers connected to the Internet, the method
4 comprising the steps of:

5 (1) posting, on an electronic list that can be viewed over the Internet,
6 information regarding one or more offers to form a contract;

7 (2) posting on the electronic list one or more responses to the one or more
8 offers;

9 (3) researching the one or more responses to determine whether they satisfy
10 one or more contract criteria;

11 (4) negotiating over the network between at least two parties to accept or
12 modify one or more of the responses; and

13 (5) electronically signing a document to consummate the contract.

14 2. The method of claim 1, wherein step (1) comprises the step of displaying
15 offers and responses in a parent-daughter spatial relationship on a computer display.

16 3. The method of claim 1, further comprising the step of sorting the one or
17 more offers and one or more responses according to a user-selected sort order.

18 4. The method of claim 1, wherein steps (1) and (2) are done anonymously,
19 such that each party to the contract cannot determine the identity of the other party
20 to the contract.

21 5. The method of claim 4, further comprising the step of simultaneous
22 revealing the identity of each party prior to step (5).

23 6. The method of claim 4, wherein steps (1) and (4) comprise the step of
24 sharing a single anonymous e-mail alias among a plurality of users.

25 7. The method of claim 1, further comprising the steps of:

26 (6) registering keywords with an electronic agent that monitors the one or
27 more offers and providing an e-mail address to be notified upon a keyword match;

28 and

29 (7) in response to the electronic agent detecting the keyword match,
30 transmitting a message to the e-mail address provided in step (6).

31 8. The method of claim 1, wherein step (2) comprises the step of clicking on
32 a hyperlink linking the information posted in step (1) to a reply card.

33 9. The method of claim 7, wherein step (2) comprises the step of requiring

1 the submission of certain information before the reply card will be accepted.

2 10. The method of claim 1, wherein steps (3) and (4) are performed a
3 plurality of times for a single contract, such that modifications are made to the one
4 or more responses.

5 11. The method of claim 1, further comprising the step of electronically
6 registering a plurality of entities that have signatory authority and correlating the
7 registered entities with one or more documents to which signatures can be affixed.

8 12. A method of displaying information on a computer display,
9 comprising the steps of:

10 (1) displaying a first plurality of graphical objects each having a shape of a
11 file folder comprising a folder face and a labeled tab, wherein the first plurality of
12 graphical objects are stacked in a cascading arrangement; and

13 (2) in response to user activation of a "flip" tab, changing the graphical
14 objects displayed in step (1) to show a second plurality of graphical objects each
15 having a shape of a file folder comprising a folder face and a labeled tab,

16 wherein each of the first and second plurality of graphical objects can be
17 brought to a foreground position in front of other graphical objects by clicking on
18 a corresponding labeled tab.

19 13. The method of claim 12, wherein each of the first and second plurality
20 of graphical objects has associated therewith one or more functions displayed on
21 the folder face thereof, wherein user can activate the one or more functions by
22 clicking thereon.

23 14. A method of creating a user-defined networked environment across a
24 plurality of computers without requiring system administrator-level privileges,
25 comprising the steps of:

26 (1) creating a group by providing a group identifier, a group description,
27 and by specifying a plurality of group members entitled to use the user-defined
28 networked environment;

29 (2) selecting a plurality of web-based communication, collaboration, and
30 transaction tools from a list of available tools, wherein the selected tools are to be
31 made available to the plurality of group members specified in claim 1; and

32 (3) through the use of computer software, automatically creating the user-
33 defined networked environment by creating a web page accessible to the plurality

1 of group members selected in step (1), wherein the web page provides access to
2 the plurality of tools selected in step (2).

3 15. The method of claim 14, wherein step (1) comprises the step of
4 inviting a plurality of individuals to join the group by transmitting an invitation to
5 prospective group members.

6 16. The method of claim 14, wherein step (1) comprises the step of
7 advertising an invitation to join the group by posting an advertisement for
8 prospective group members, wherein at least some of the prospective group
9 members are unknown to the user creating the networked environment.

10 17. The method of claim 14, further comprising the step of screening
11 prospective members that respond to the advertisement in order to determine
12 whether they should be added to the group.

13 18. The method of claim 14, further comprising the steps of electronically
14 collaborating among group members using the user-defined networked
15 environment.

16 19. The method of claim 14, further comprising the step of destroying the
17 user-defined networked environment when it is no longer needed.

18 20. The method of claim 14, wherein step (2) comprises the step of
19 selecting a transaction engine that implements an auction to members of the
20 group.

21 21. The method of claim 14, wherein step (2) comprises the step of
22 selecting a transaction engine that implements an on-line electronic survey
23 comprising survey questions that are to be answered electronically by survey
24 participants.

25 22. The method of claim 14, wherein step (2) comprises the step of
26 selecting a transaction engine that implements a bid-and-proposal tool that permits
27 group members to electronically submit bids on one or more proposals.

28 23. The method of claim 14, wherein step (2) comprises the step of
29 selecting an online ordering engine that permits group members to electronically
30 order goods or services in the user-defined networked environment.

31 24. The method of claim 14, wherein step (2) comprises the step of
32 selecting an Electronic Data Interchange (EDI) compatible interface that executes
33 electronic commercial transactions between two or more group members.

1 25. The method of claim 14, wherein step (2) comprises the step of a
2 selecting an electronic brain-writing tool that permits participants to brainstorm
3 using electronic idea cards.

4 26. A system for implementing a user-defined networked environment
5 that can be created without the need for system administrator-level privileges,
6 comprising:

7 a plurality of networked computers that communicate using Internet
8 Protocol;

9 a plurality of web browsers executing on the plurality of networked
10 computers;

11 a database that stores information concerning the user-defined networked
12 environment; and

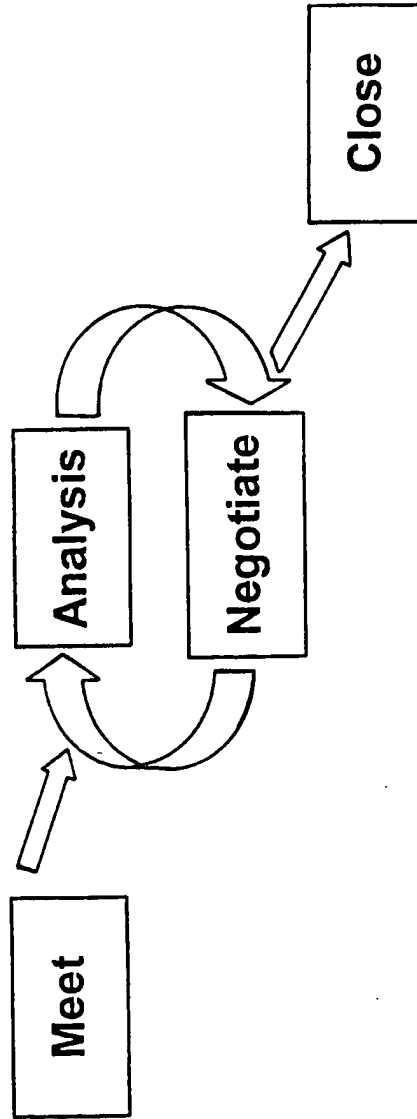
13 a computer program executing on one or more of the plurality of
14 networked computers, wherein the computer program performs the steps of:

15 (1) permitting a user to create a group comprising a plurality of group
16 members;

17 (2) permitting the user to select a plurality of web-based communication,
18 collaboration, and transaction tools from a list of available tools, wherein the
19 selected tools are to be made available to the plurality of group members; and

20 (3) automatically generating a web page accessible to the plurality of
21 group members, wherein the web page provides access to the plurality of tools
22 selected in step (2) to the plurality of group members.

FIG. 1A



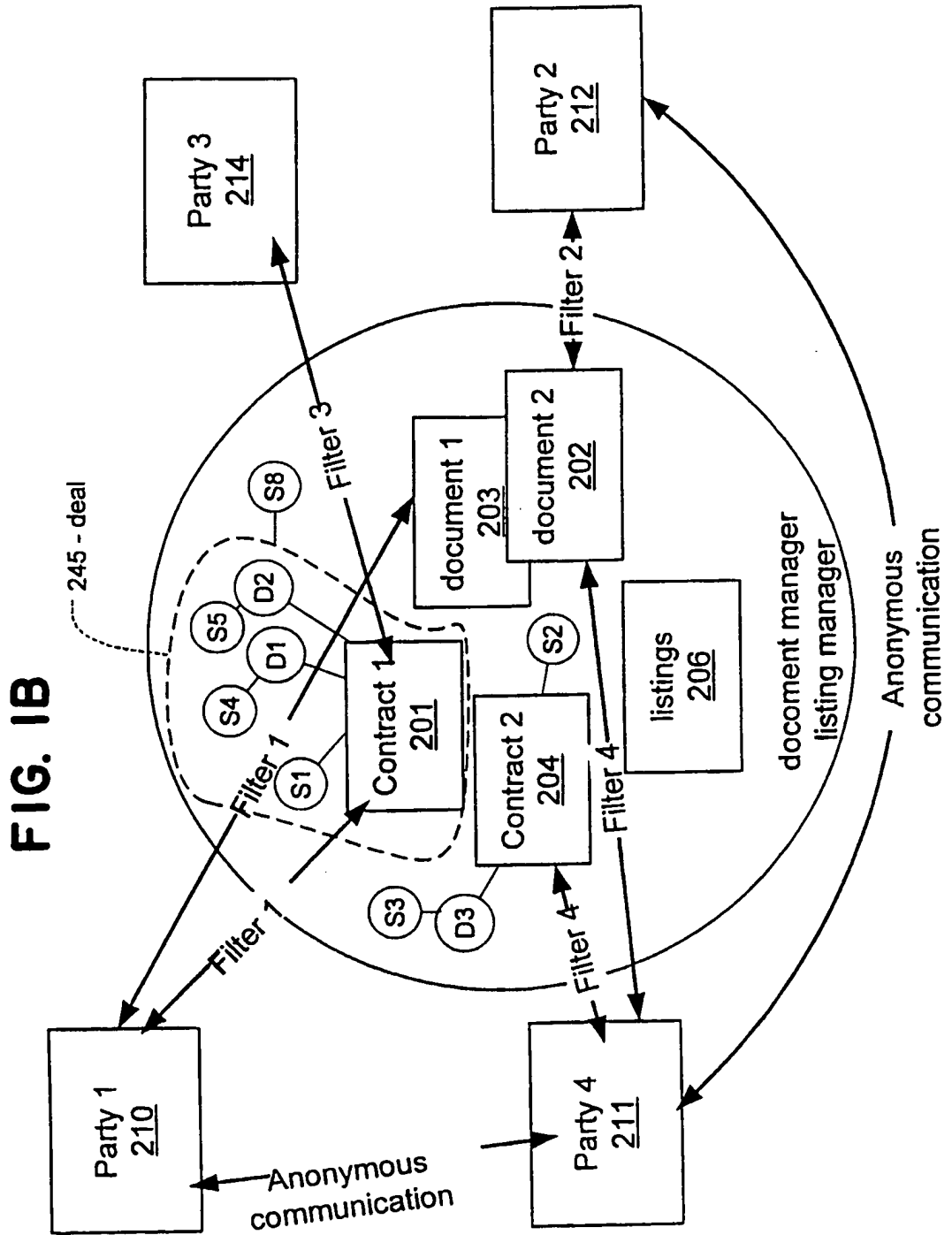


FIG. 2

Number	Date	Market	Action	Title
<u>123</u>	7/10/87	Steel	Buy	Title
<u>234</u>	7/12/87	Alum.	Sell	Title
<u>236</u>	7/12/87			Title
<u>239</u>	7/10/88	Gold	Action	Title
<u>240</u>	8/12/87	Flood	Action	Title
<u>243</u>	9/01/87		Action	Title

SUBSTITUTE SHEET (RULE 26)

FIG. 3

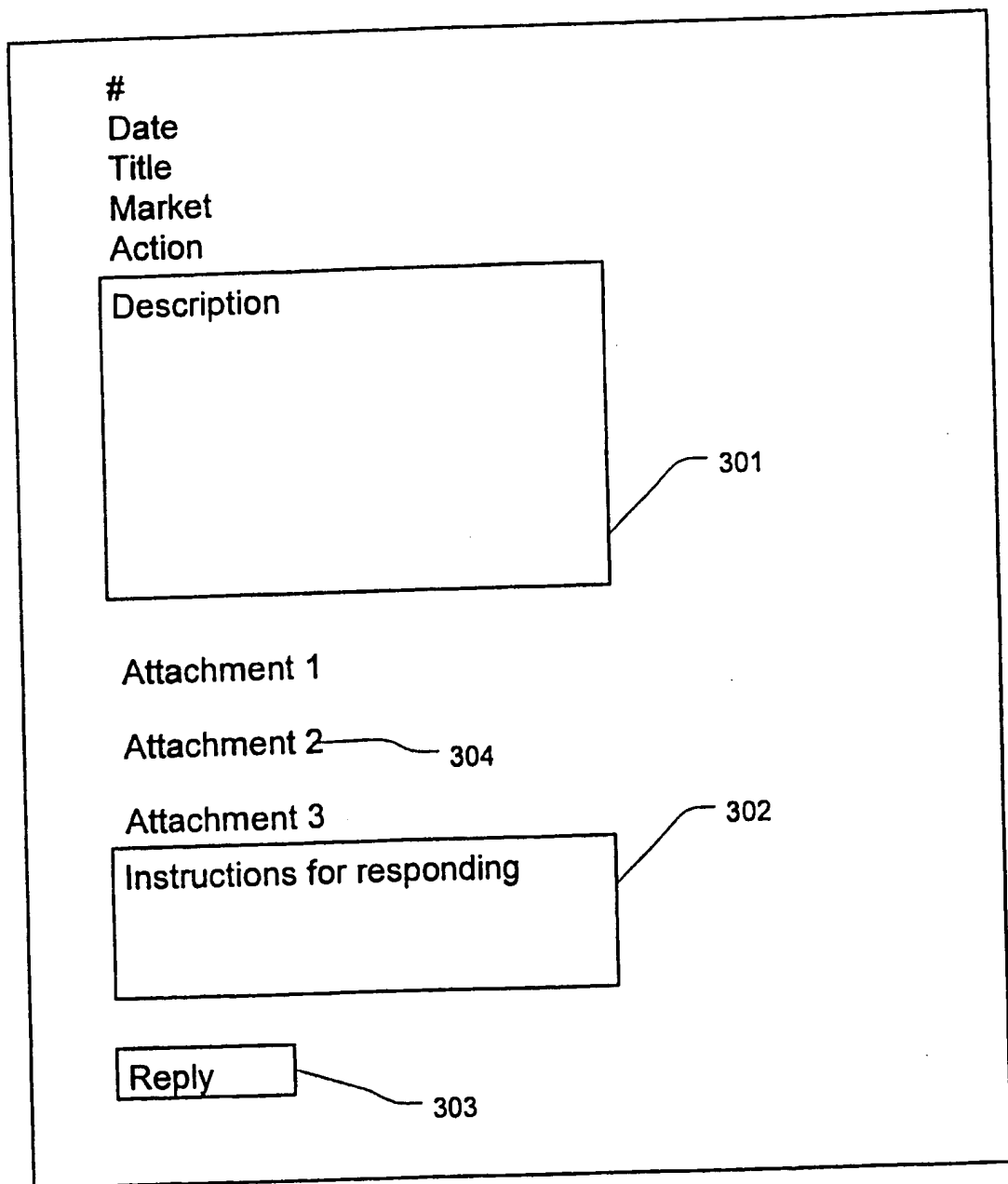


FIG. 4

Reply to Listing 145: Request for Bid on School Construction

Name of Company

Address

D&B Number

References for Construction Work in Fairfax County

Do you qualify as a:

Small Business

Minority owned business

Woman owned business

SUBSTITUTE SHEET (RULE 26)

6/31

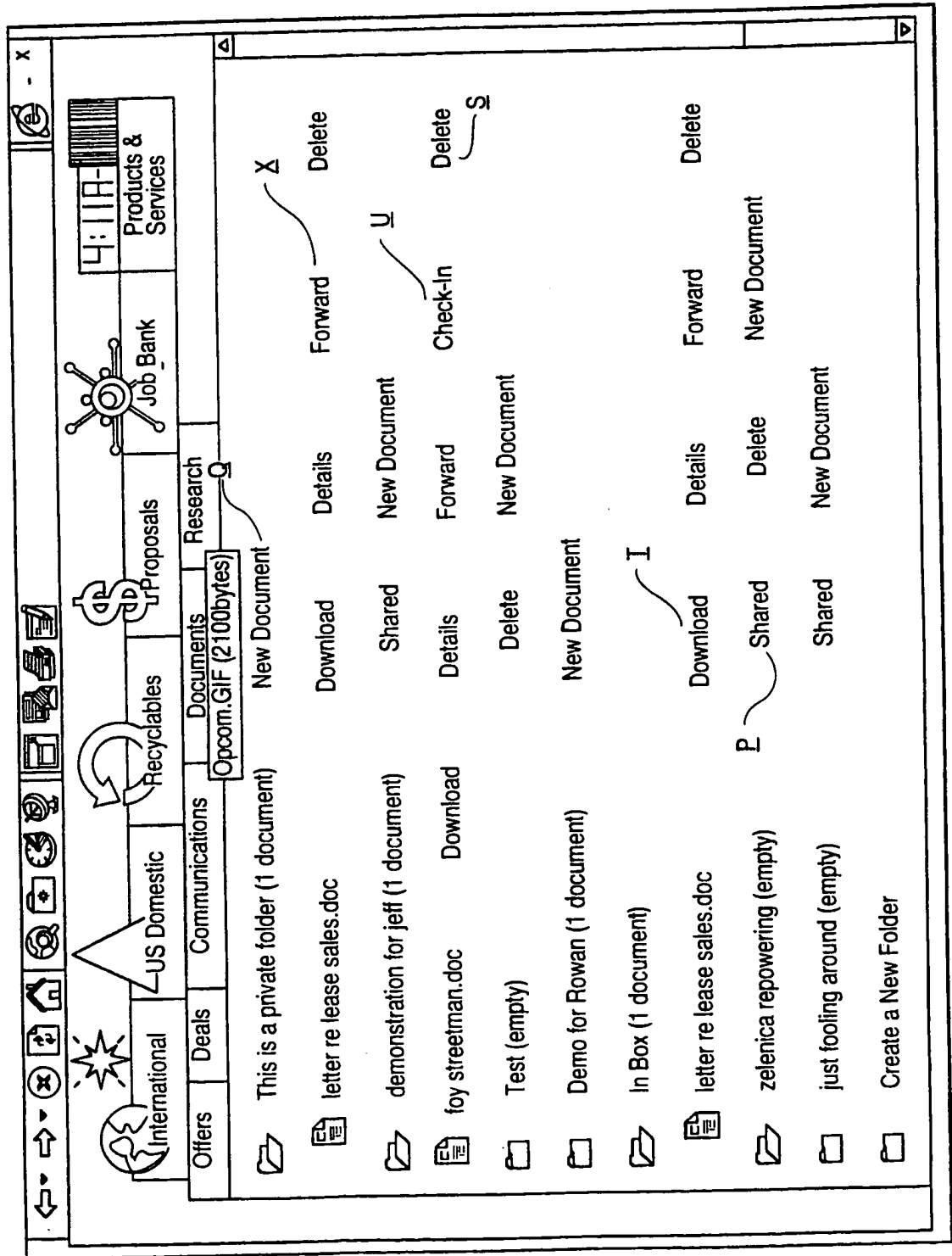


FIG. 5

SUBSTITUTE SHEET (RULE 26)

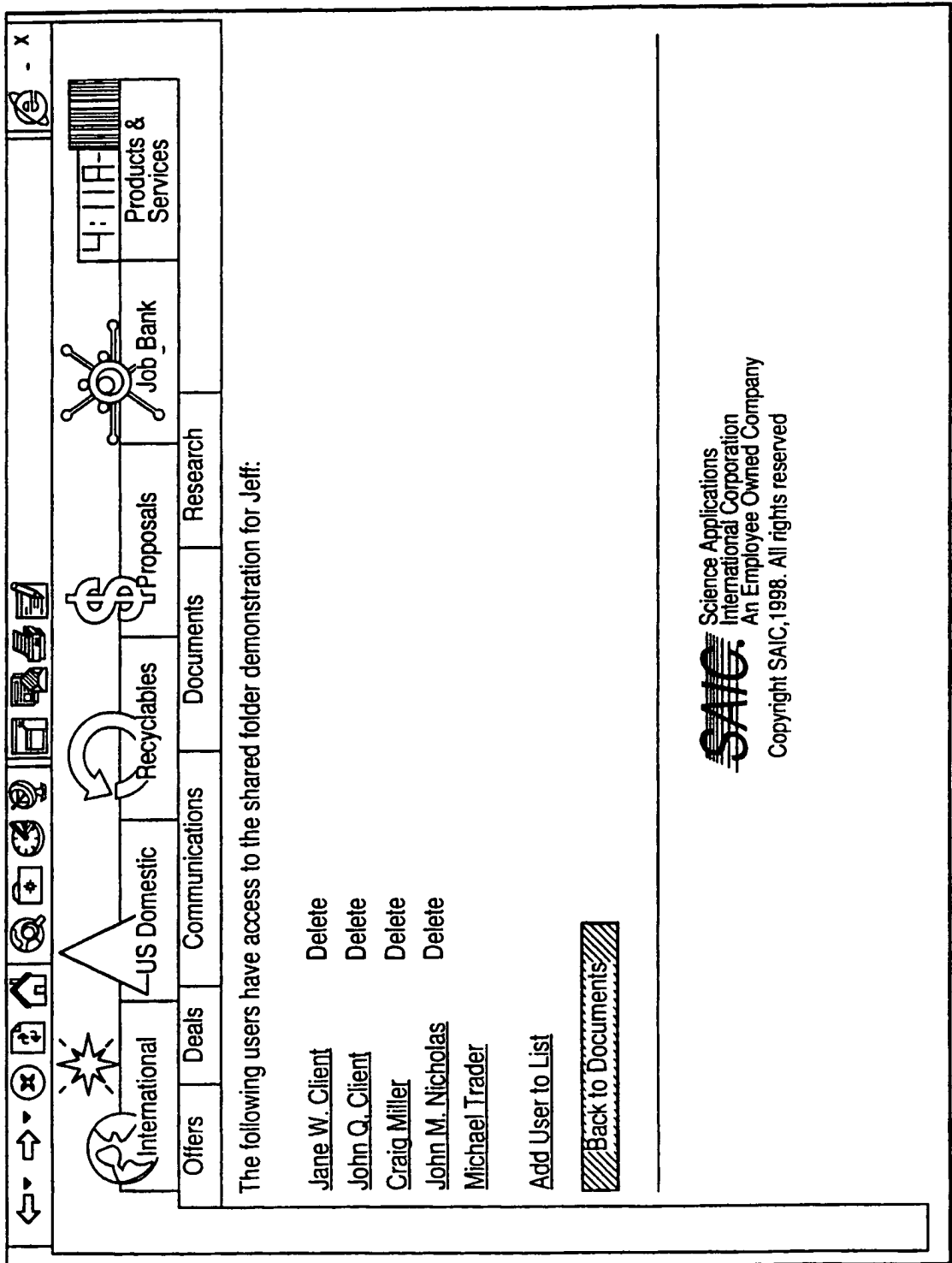


FIG. 6

8/31

Trade Number	Date Created	Trade Title
357	Sep 22 1998	mmmmmmmmmm
356	Sep 22 1998	World Trade Center
353	Sep 22 1998	Florida Windstorm Coverage
352	Sep 22 1998	www
342	Sep 1 1998	Bigger deal
341	Sep 1 1998	big deal
330	Aug 18 1998	Another trade
297	Jun 23 1998	xgssgs
295	Jun 23 1998	lkjdalskj
293	Jun 23 1998	Test again
292	Jun 23 1998	Test of compiled tm
6	Feb 11 1998	Get in shape
5	Feb 10 1998	Big Deal
4	Feb 8 1998	Master Contract

FIG. 7

SUBSTITUTE SHEET (RULE 26)

SAIC
 Science Applications
 International Corporation
 An Employee Owned Company
 Copyright SAIC, 1998. All rights reserved

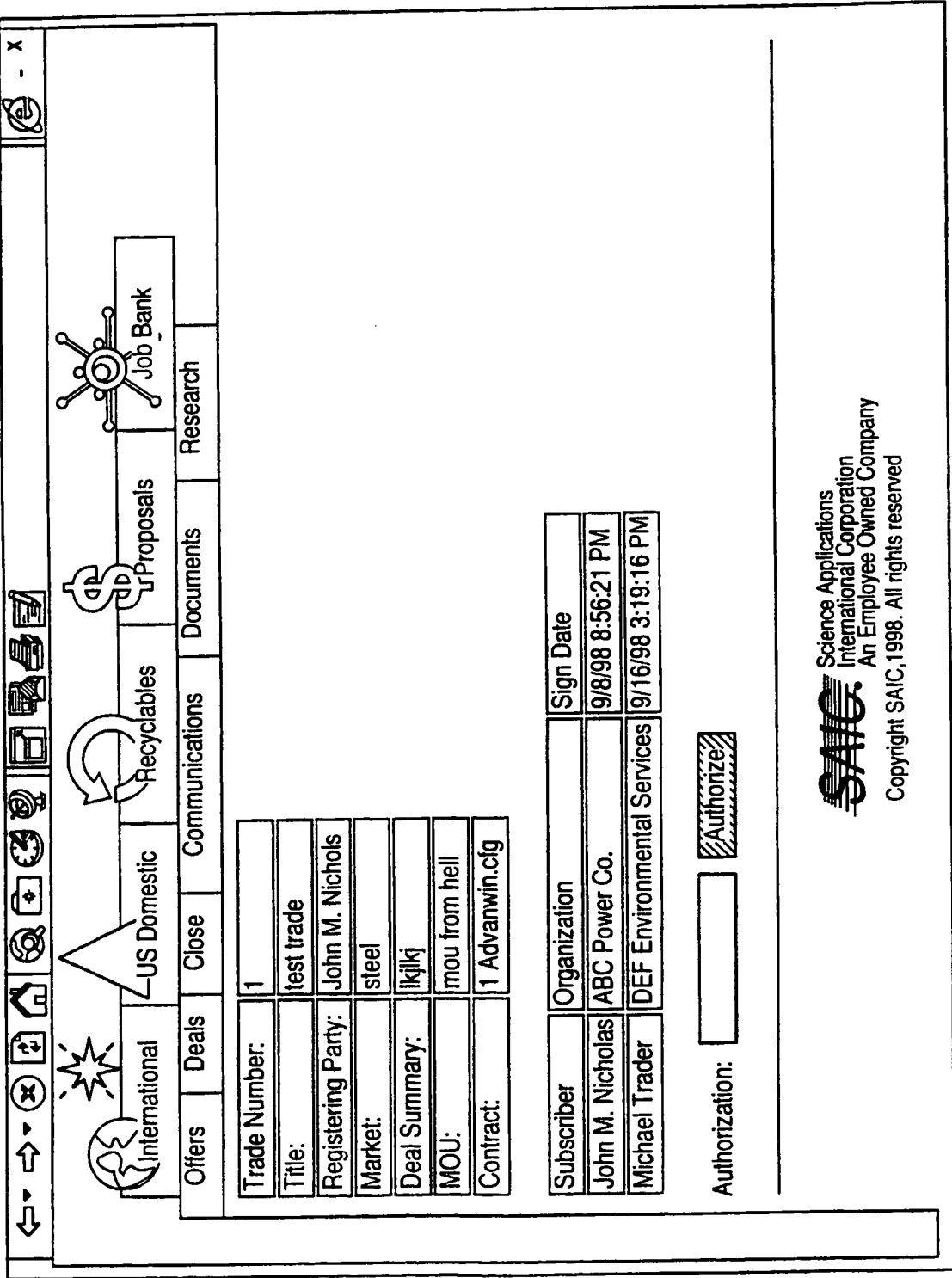


FIG. 8A

SUBSTITUTE SHEET (RULE 26)

SAIC
 Science Applications
 International Corporation
 An Employee Owned Company
 Copyright SAIC, 1998. All rights reserved

Specify Title, Rate Summary, Deal Summary, Slip Sheet, Exhibits, and Authorizing Parties

Title:

Rate Summary:

Deal Summary:

Slip Sheet:

Add Exhibit: Browse

Description:

Add Exhibit: Browse

Description:

Specify Parties who will Authorize the Deal

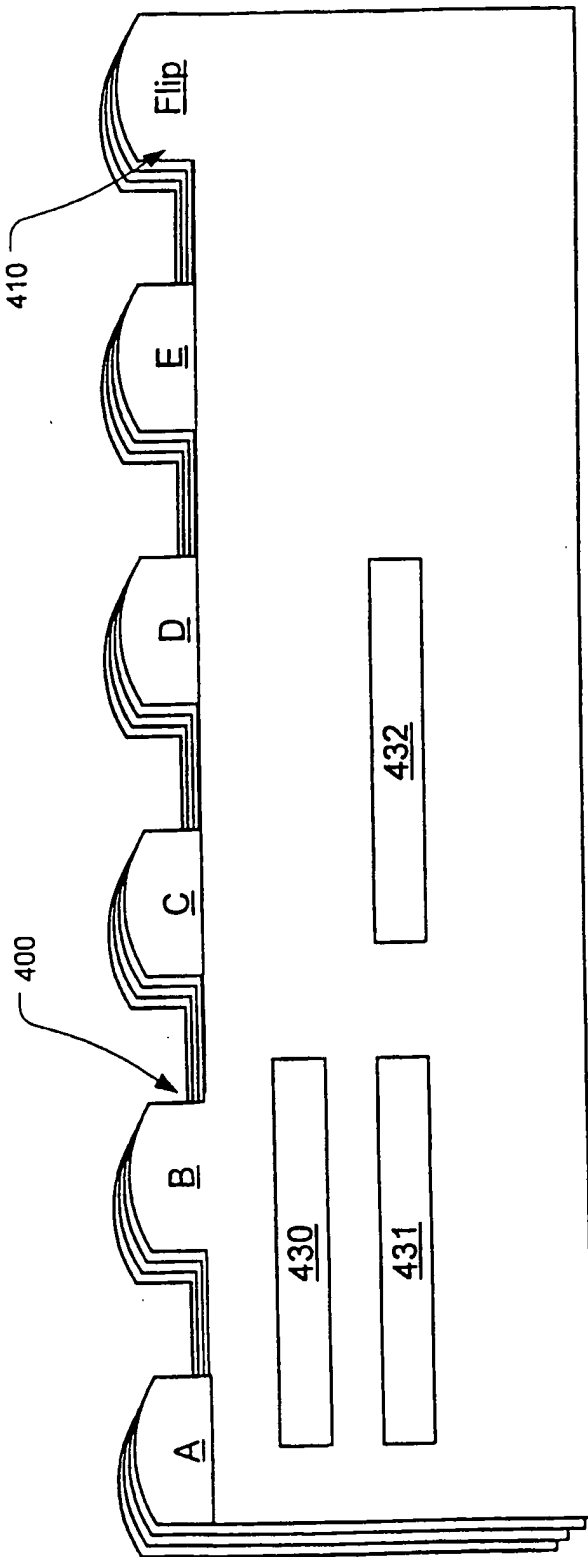
Company: Add Delete

Names: Authorizing Parties:

FIG. 8B

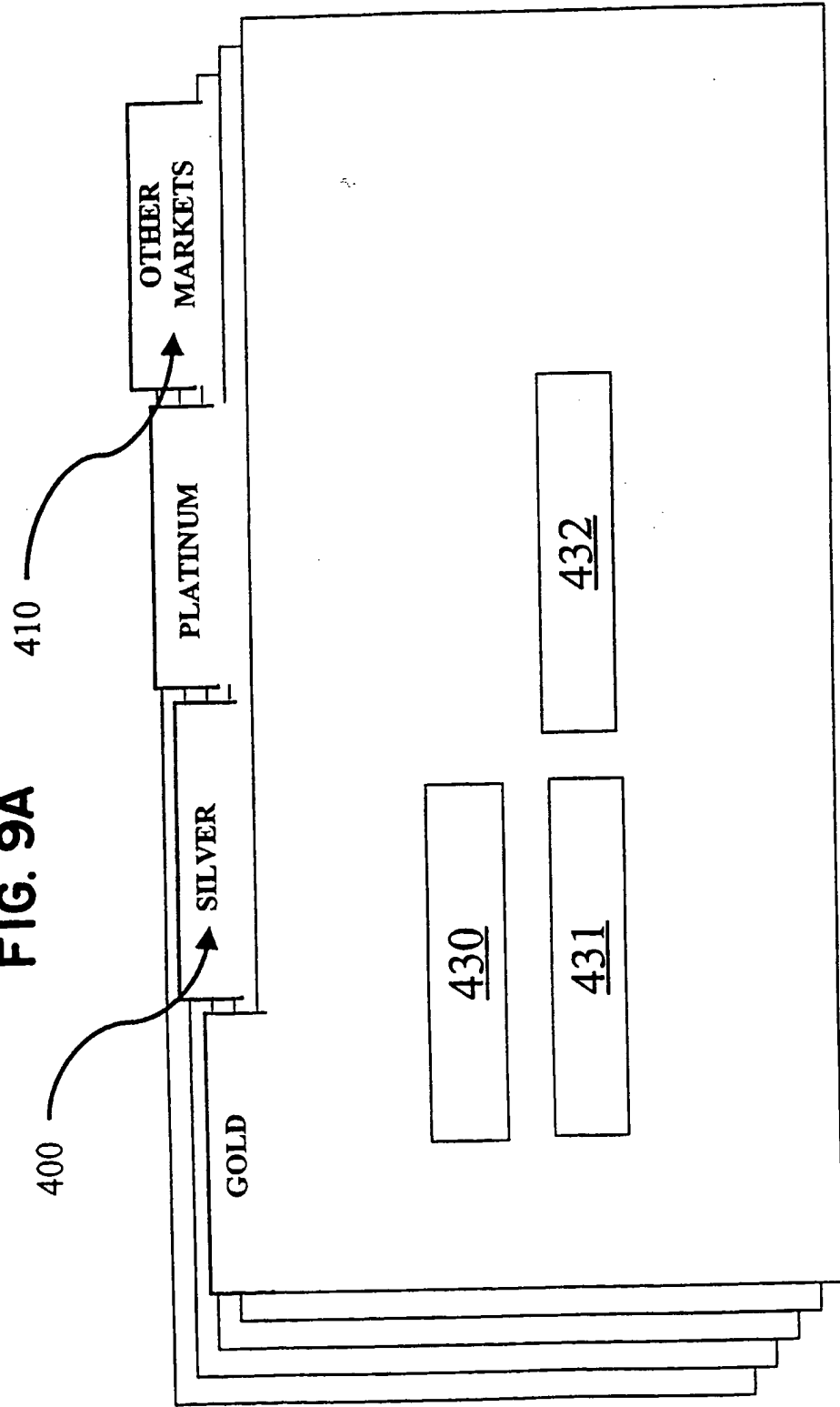
11/31

FIG. 9



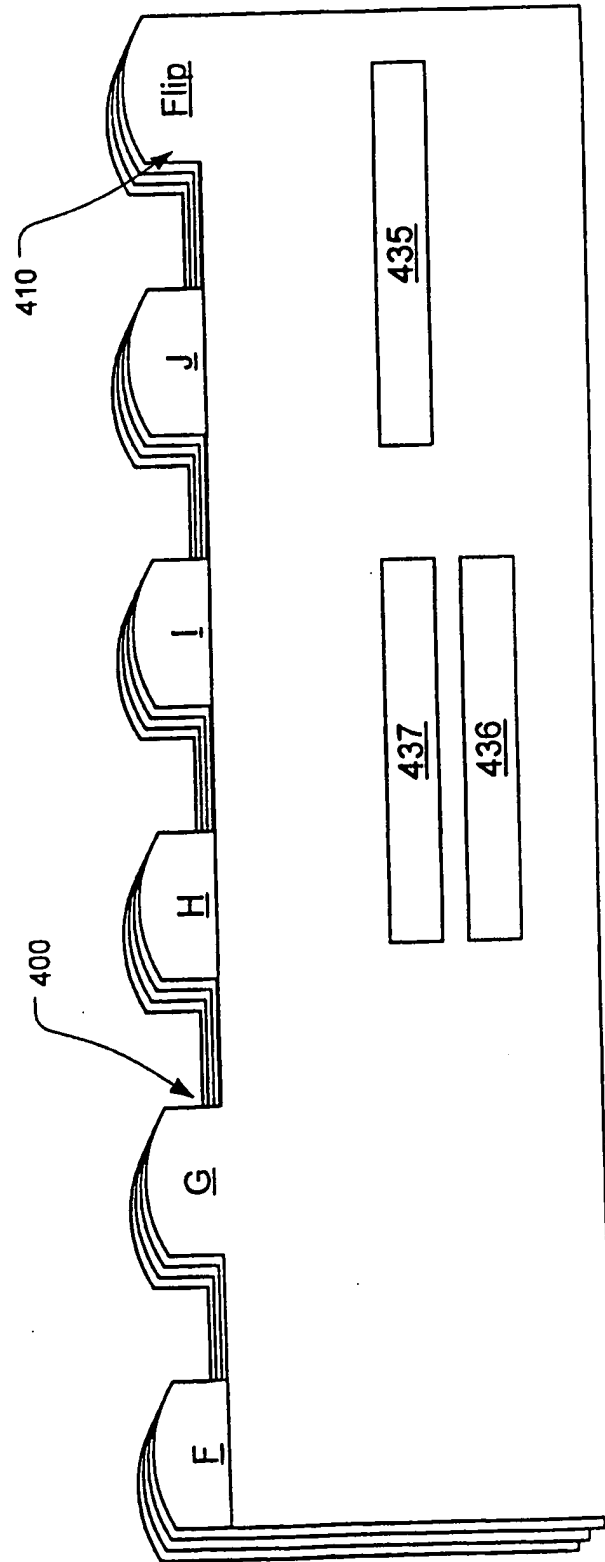
SUBSTITUTE SHEET (RULE 26)

FIG. 9A



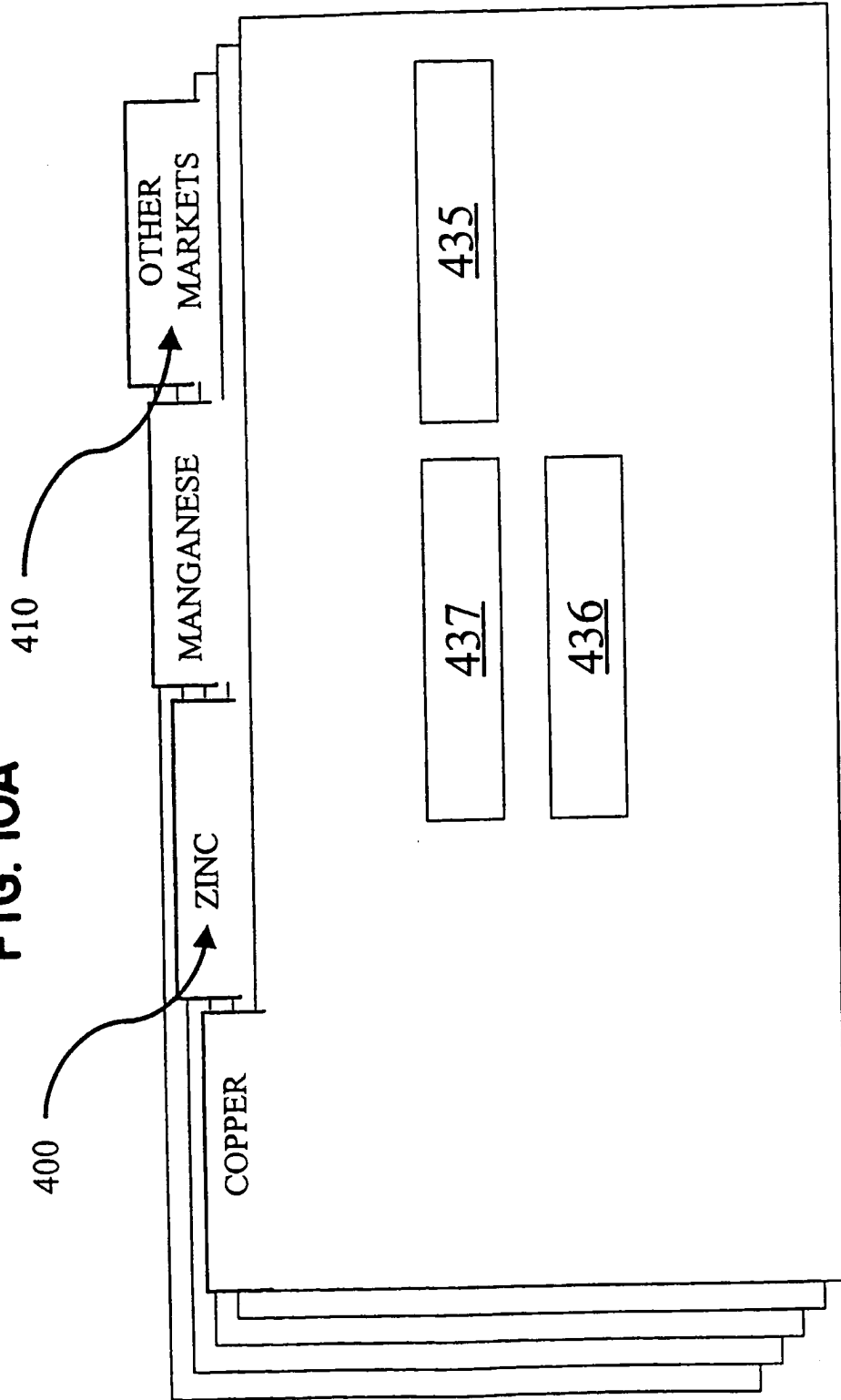
SUBSTITUTE SHEET (RULE 26)

FIG. 10

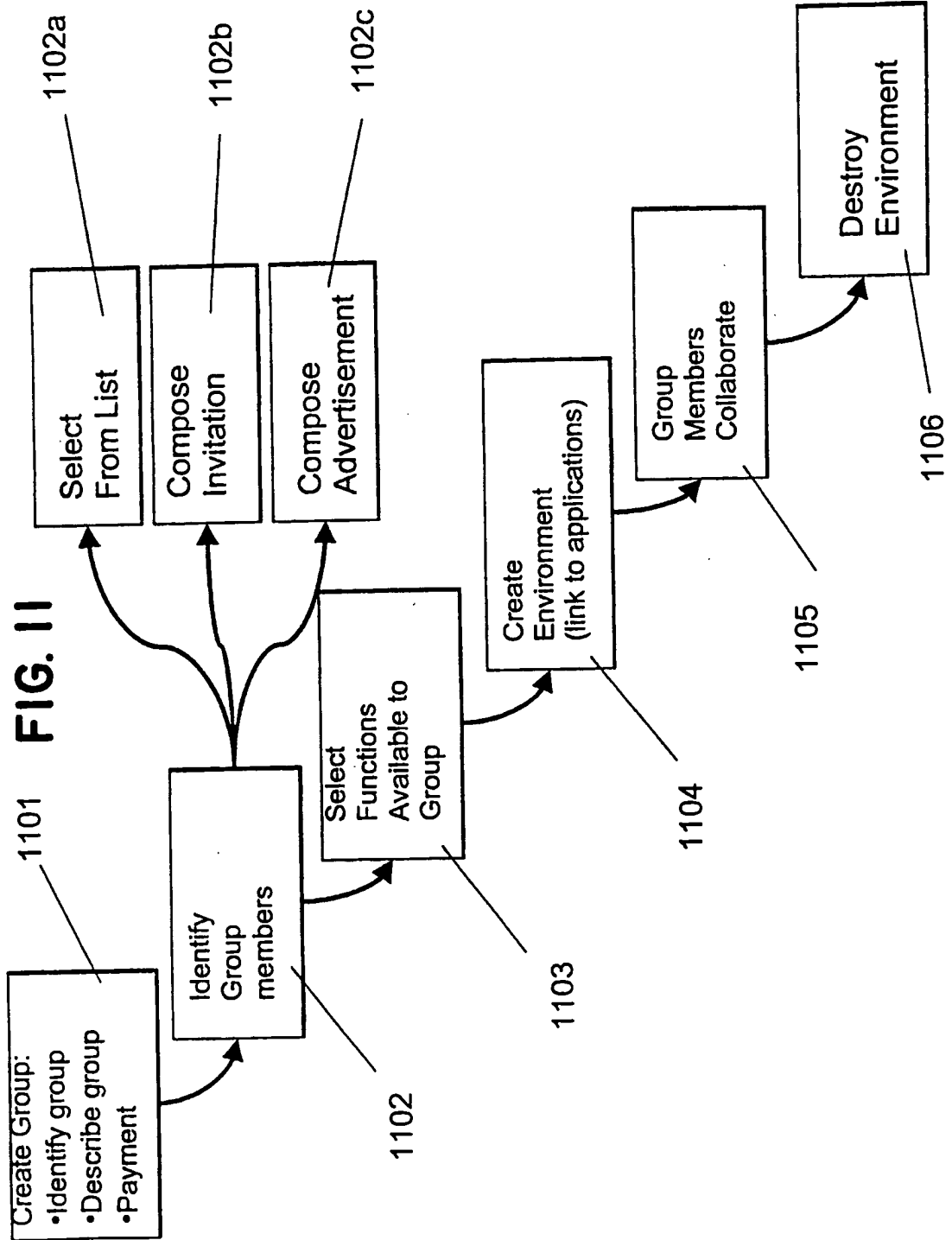


SUBSTITUTE SHEET (RULE 26)

FIG. 10A



SUBSTITUTE SHEET (RULE 26)



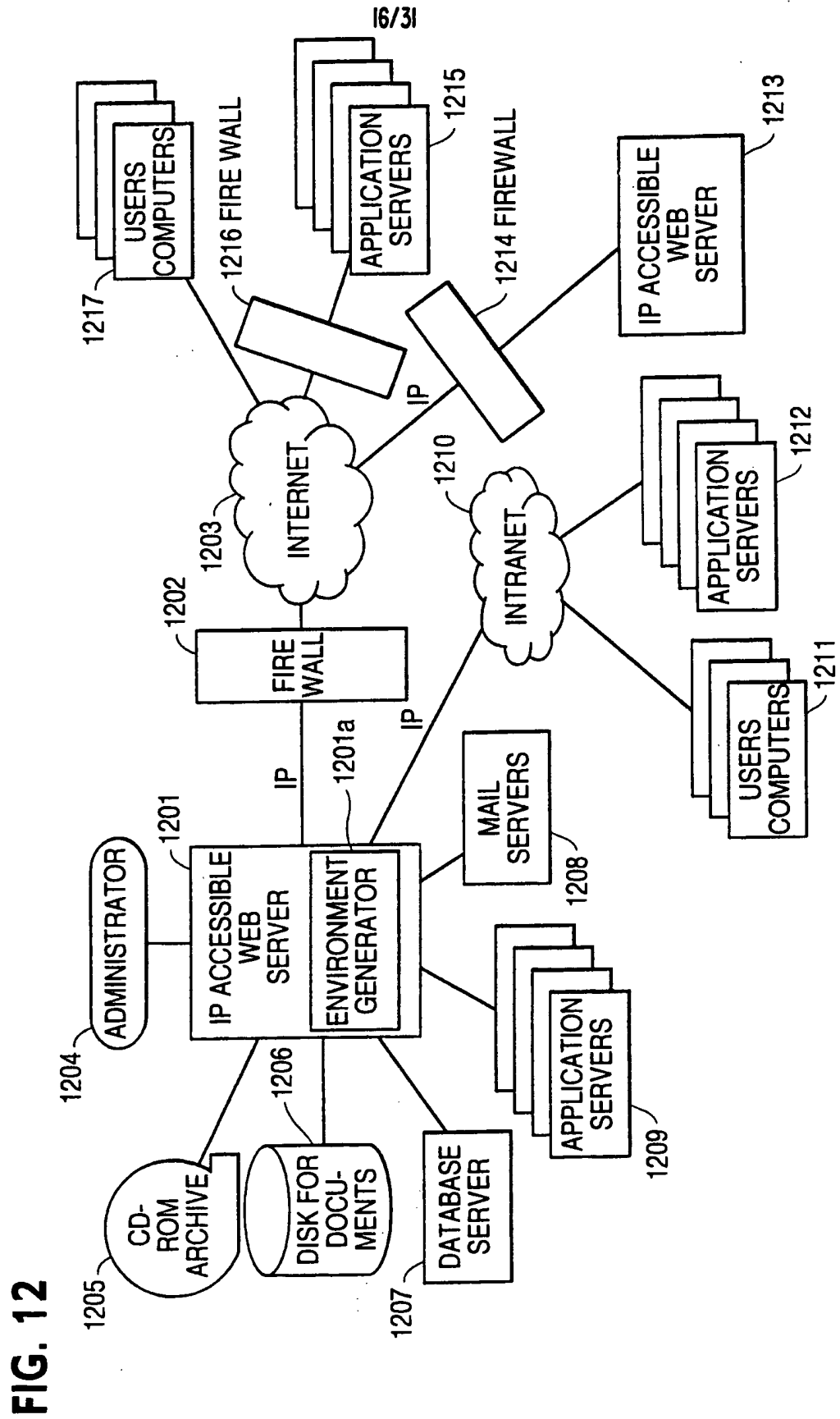


FIG. 12

SUBSTITUTE SHEET (RULE 26)

FIG. 13A

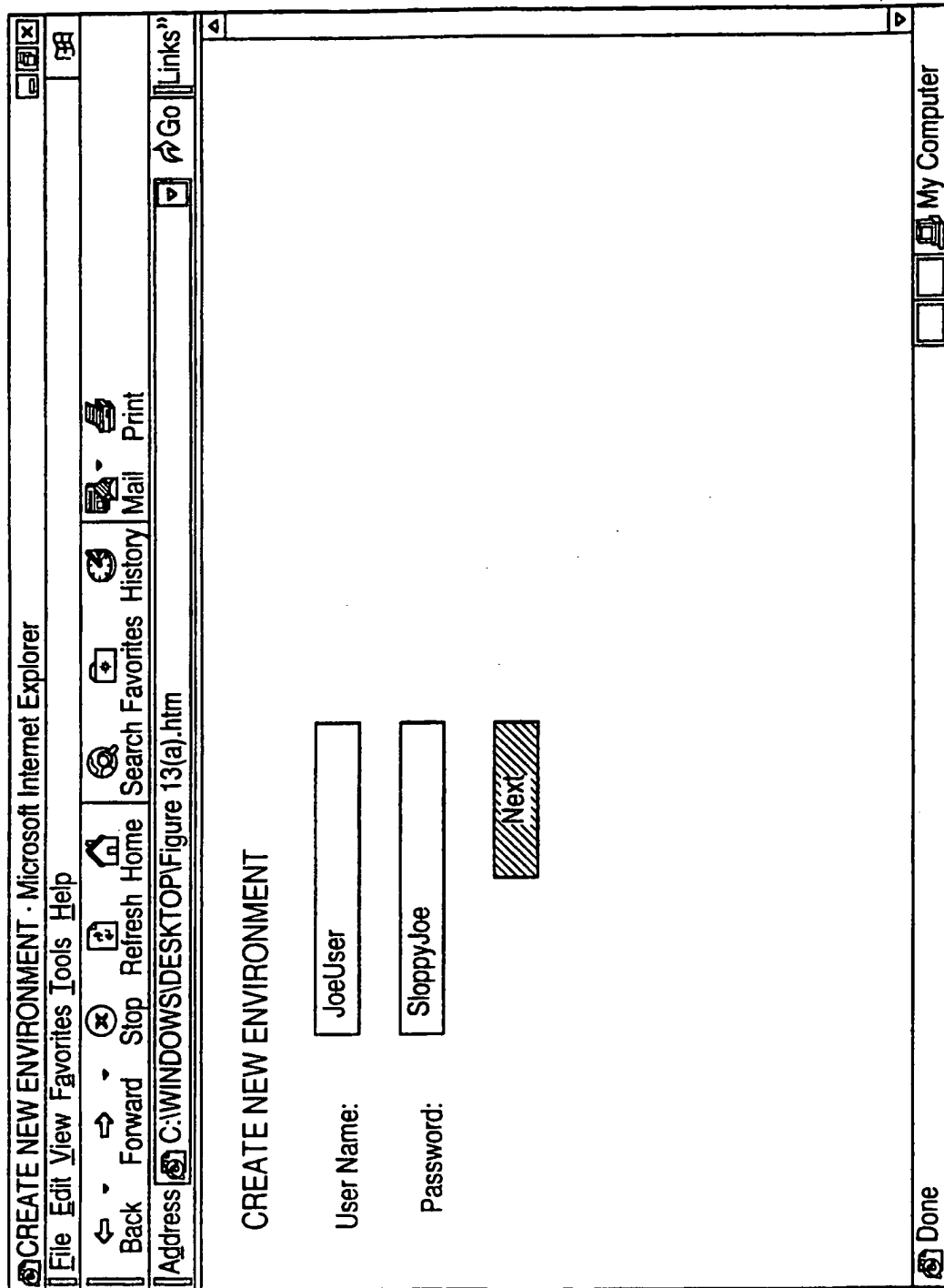


FIG. 13B

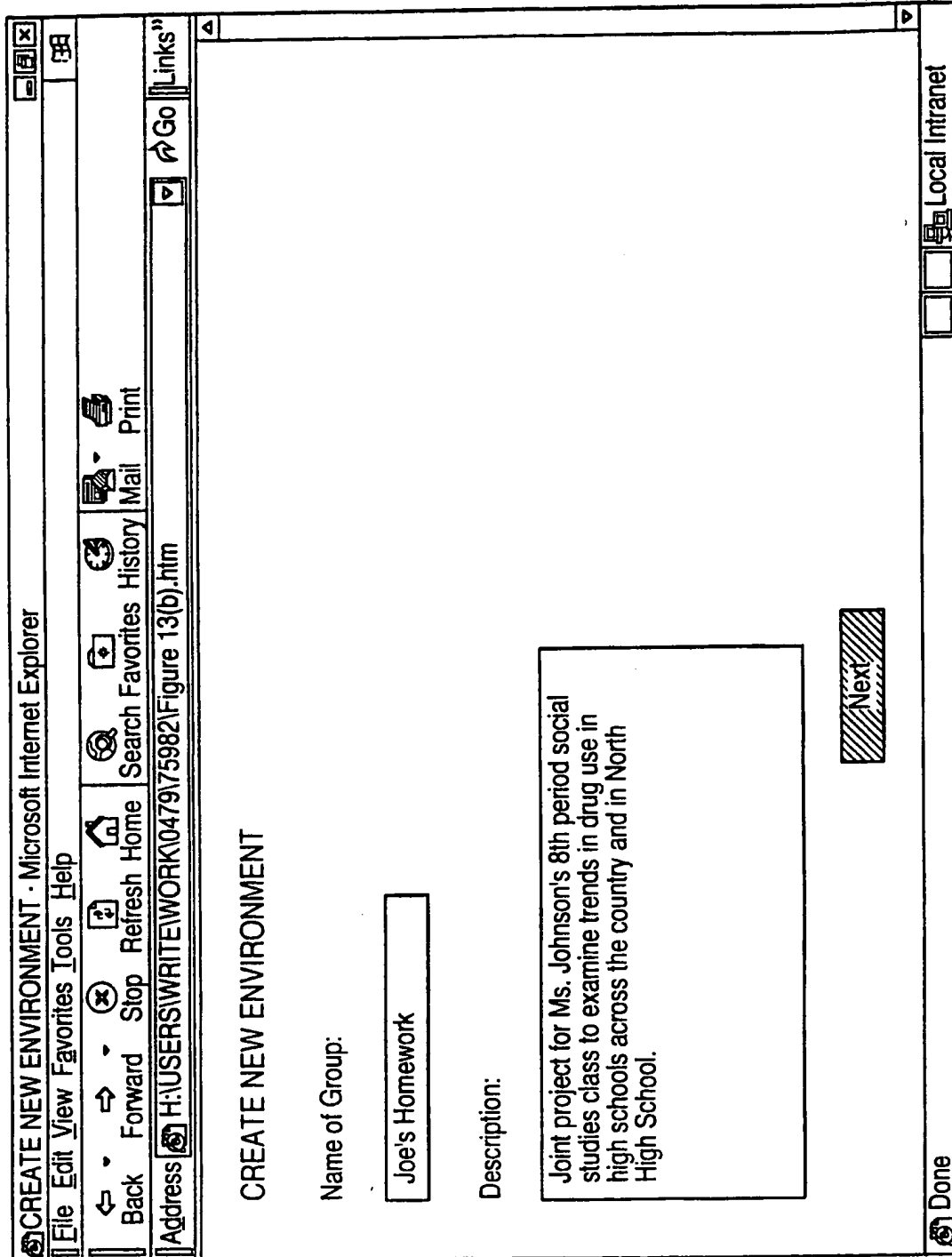


FIG. 13C

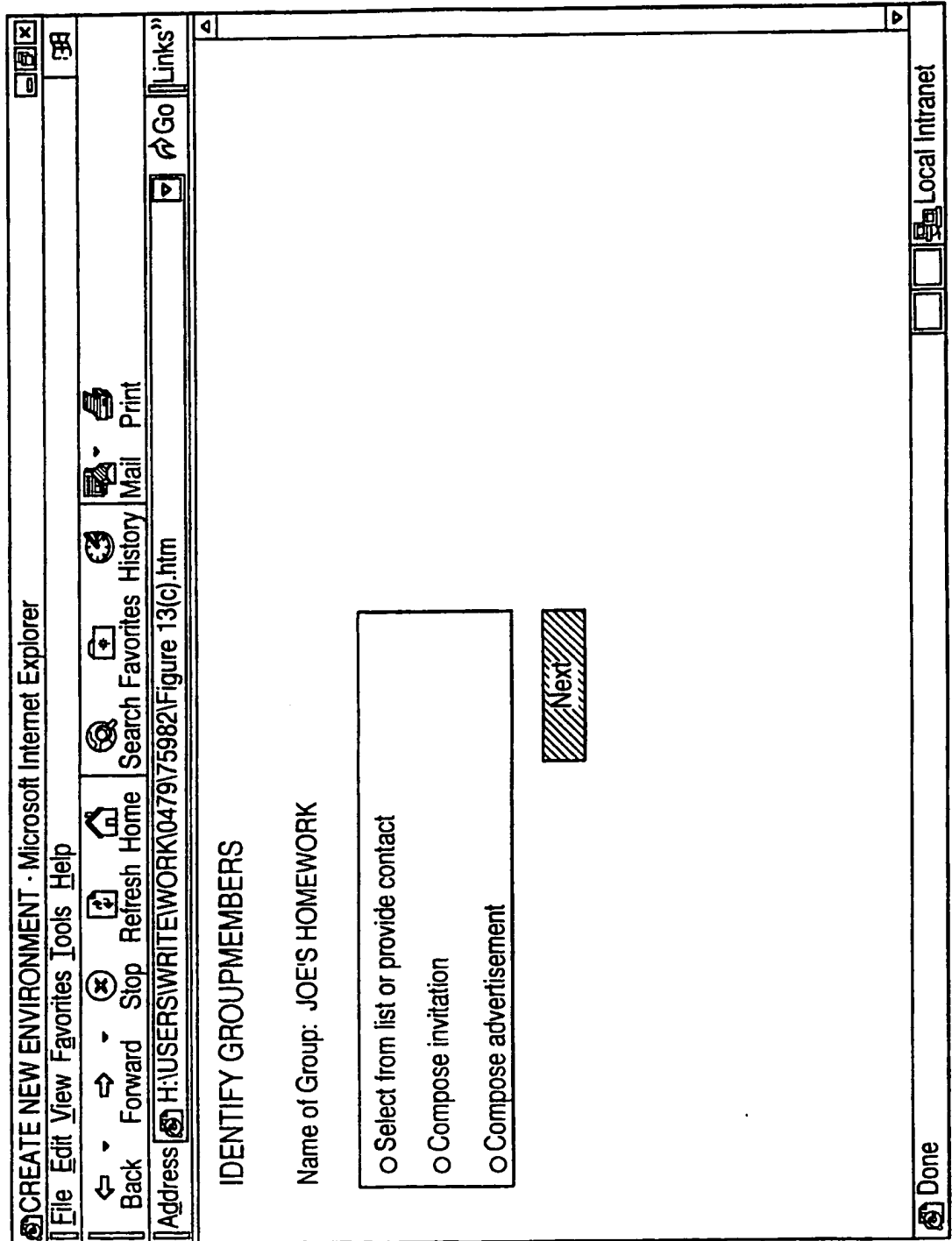


FIG. 14A

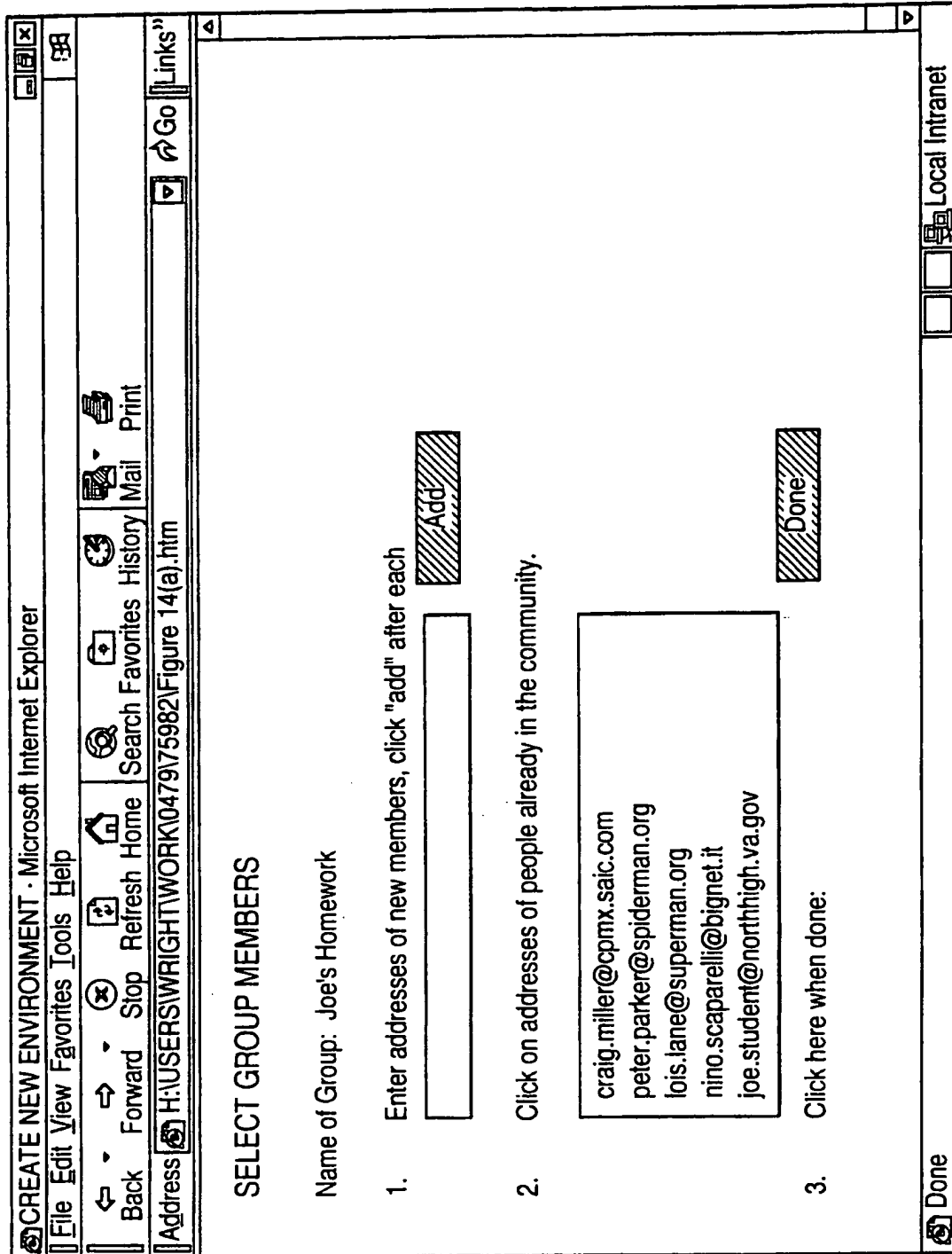
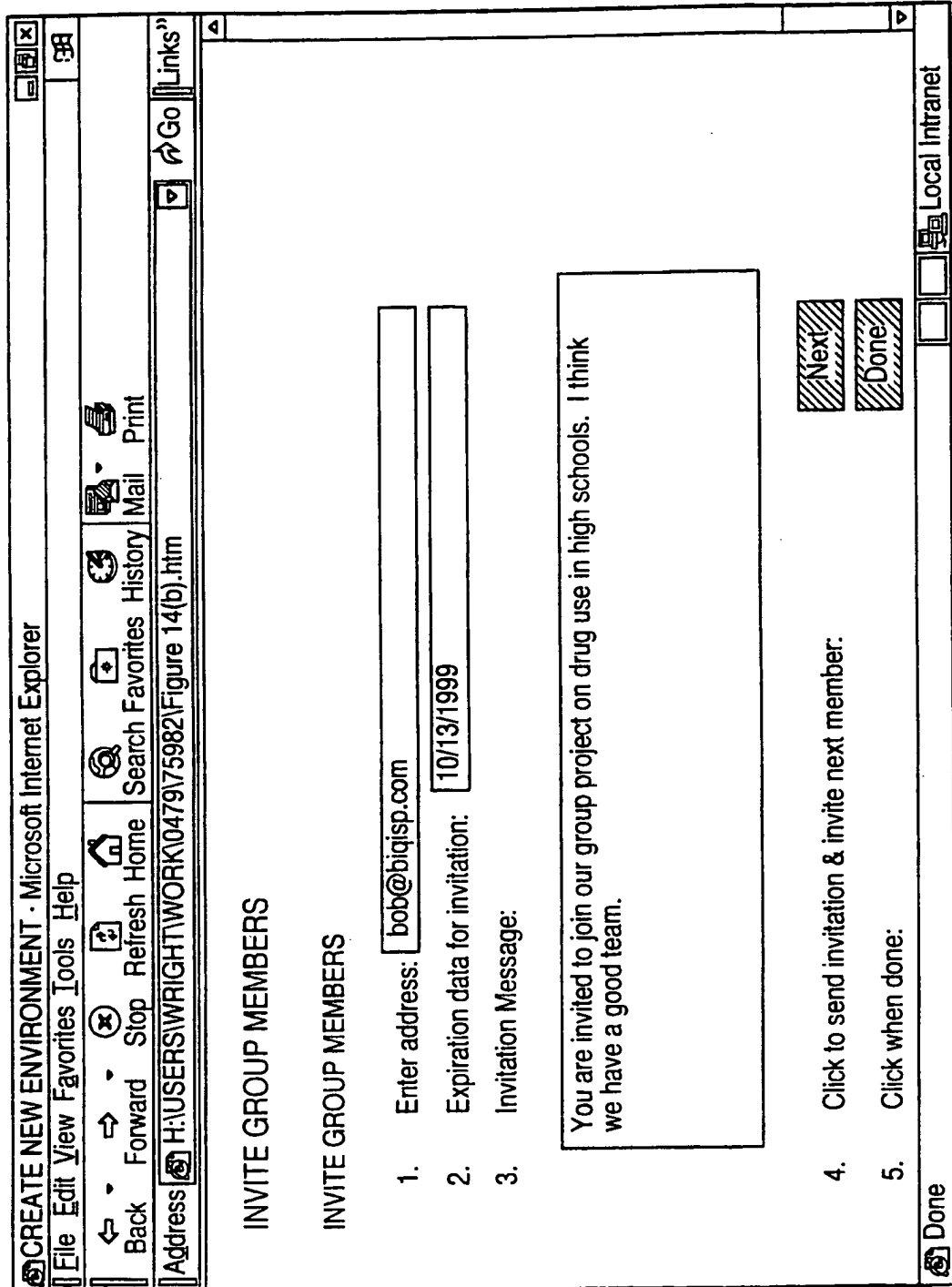


FIG. 14B



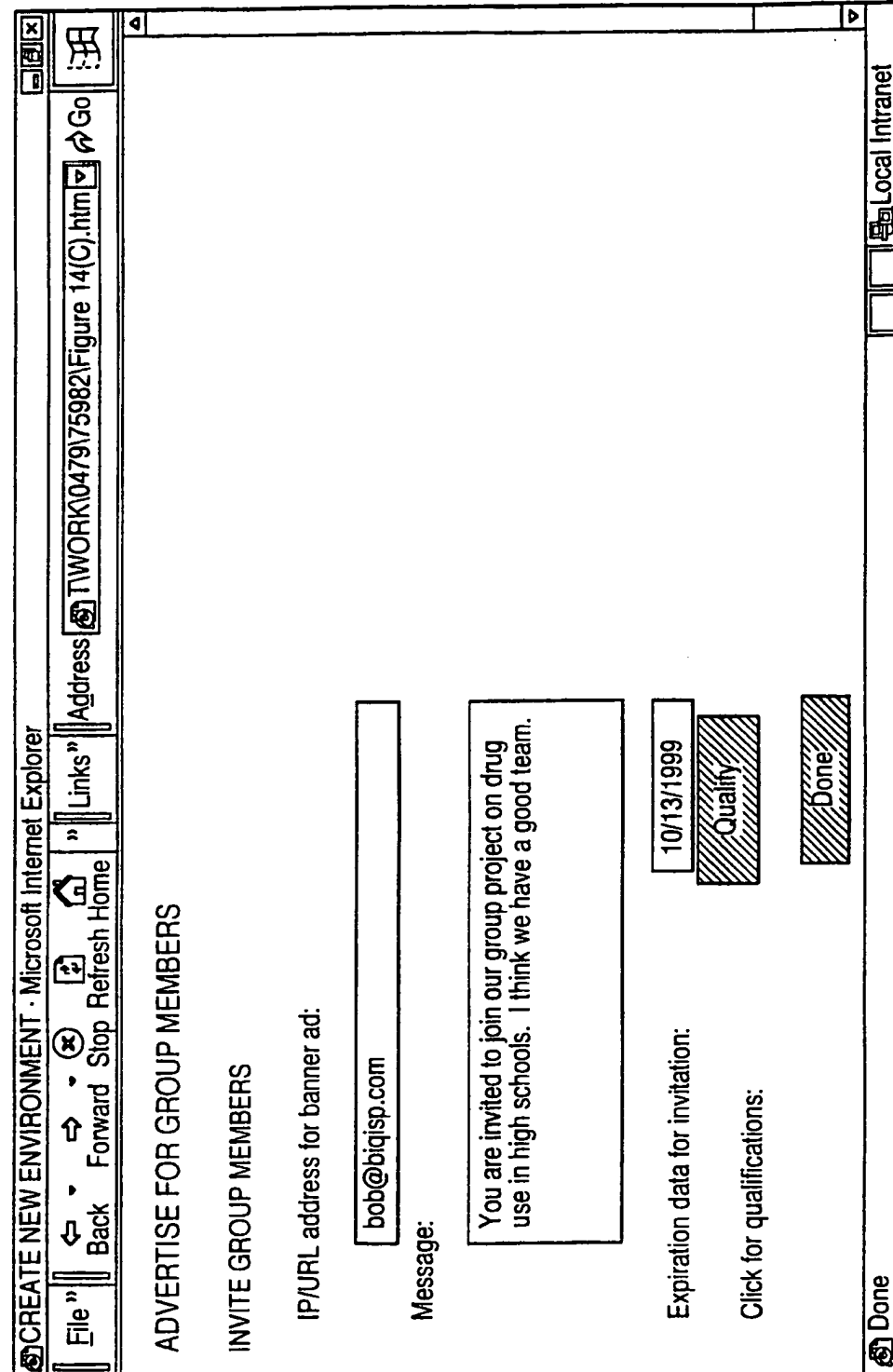


FIG. 14C

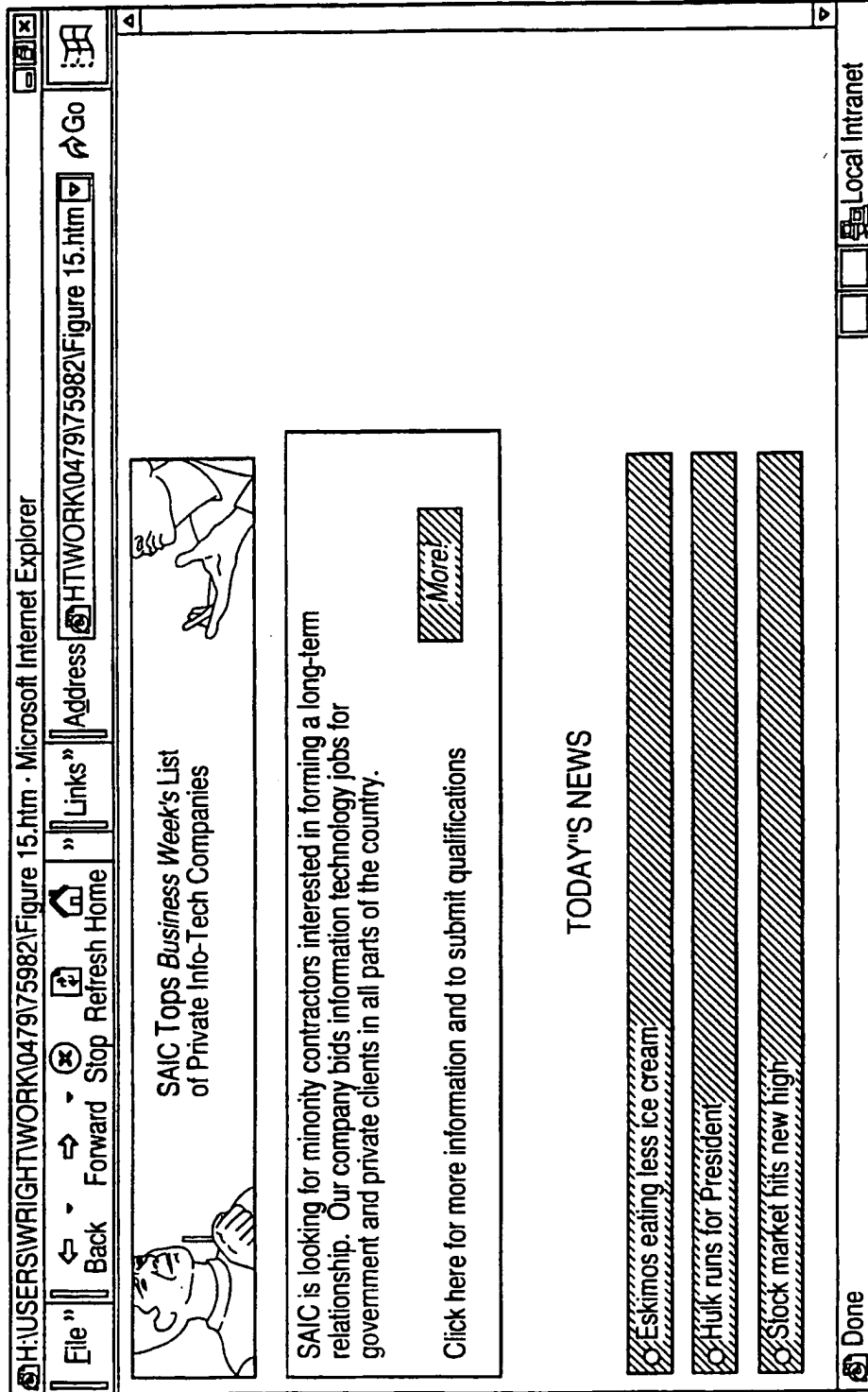


FIG. 15

SUBSTITUTE SHEET (RULE 26)

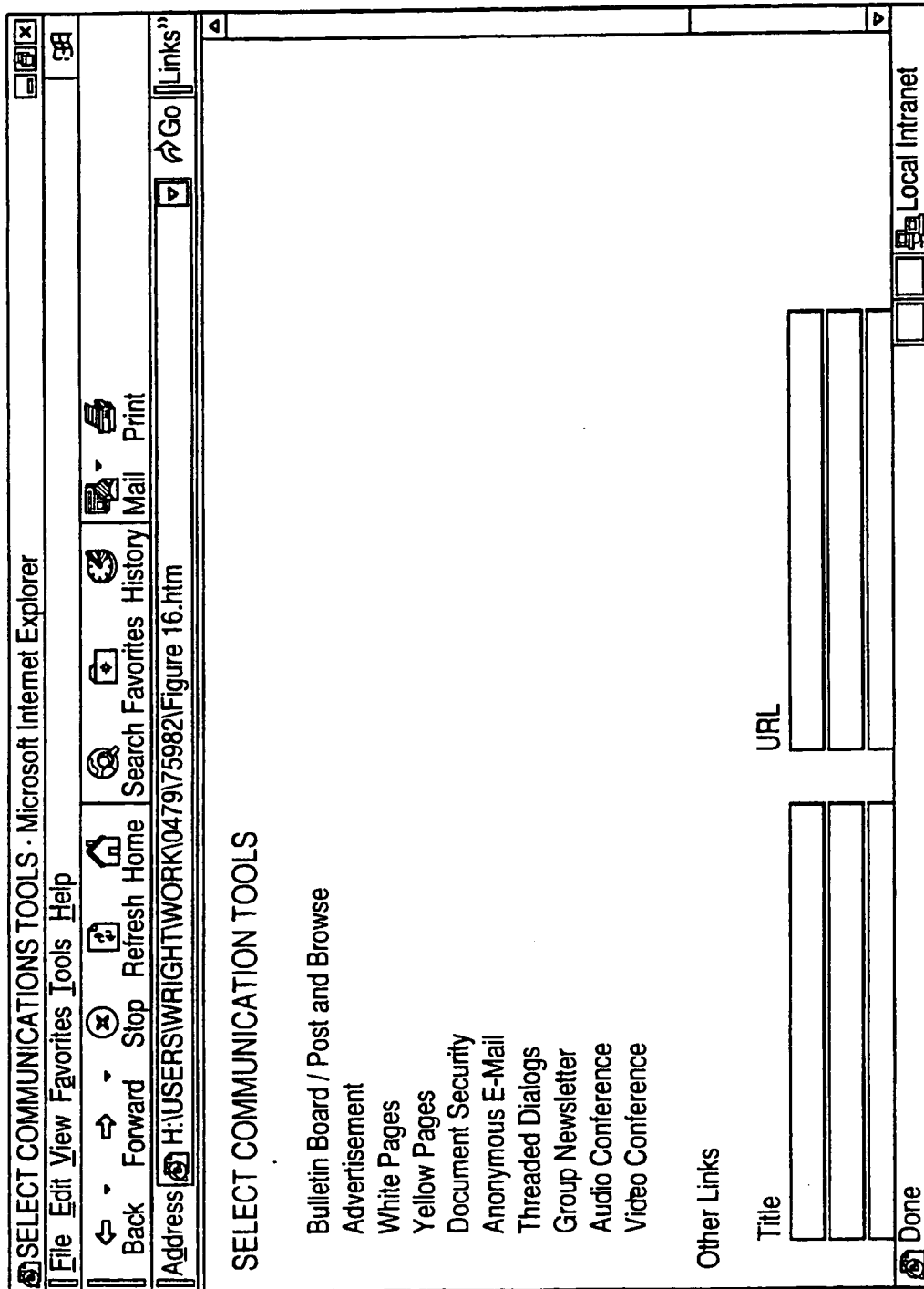


FIG. 16

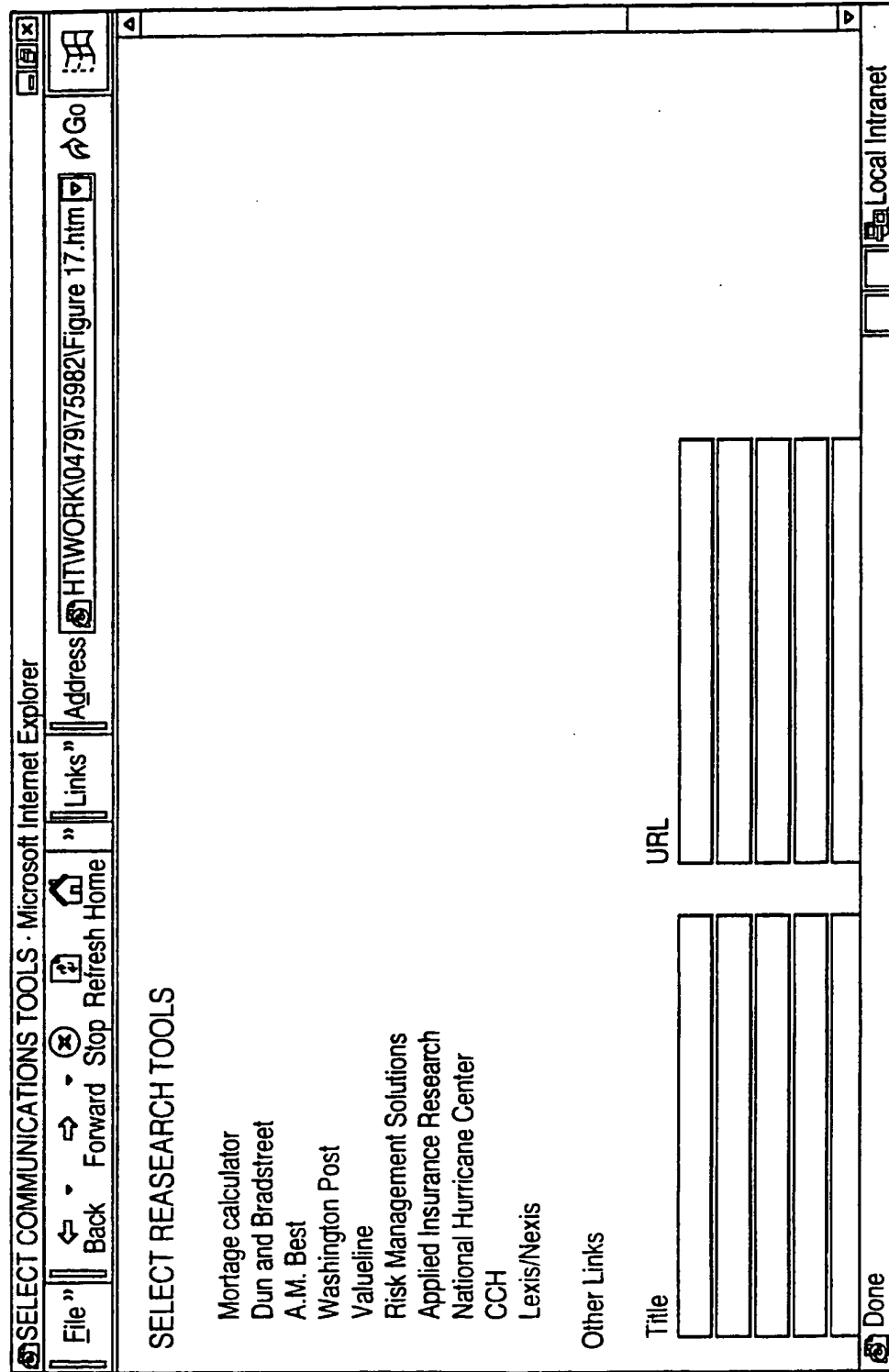


FIG. 17

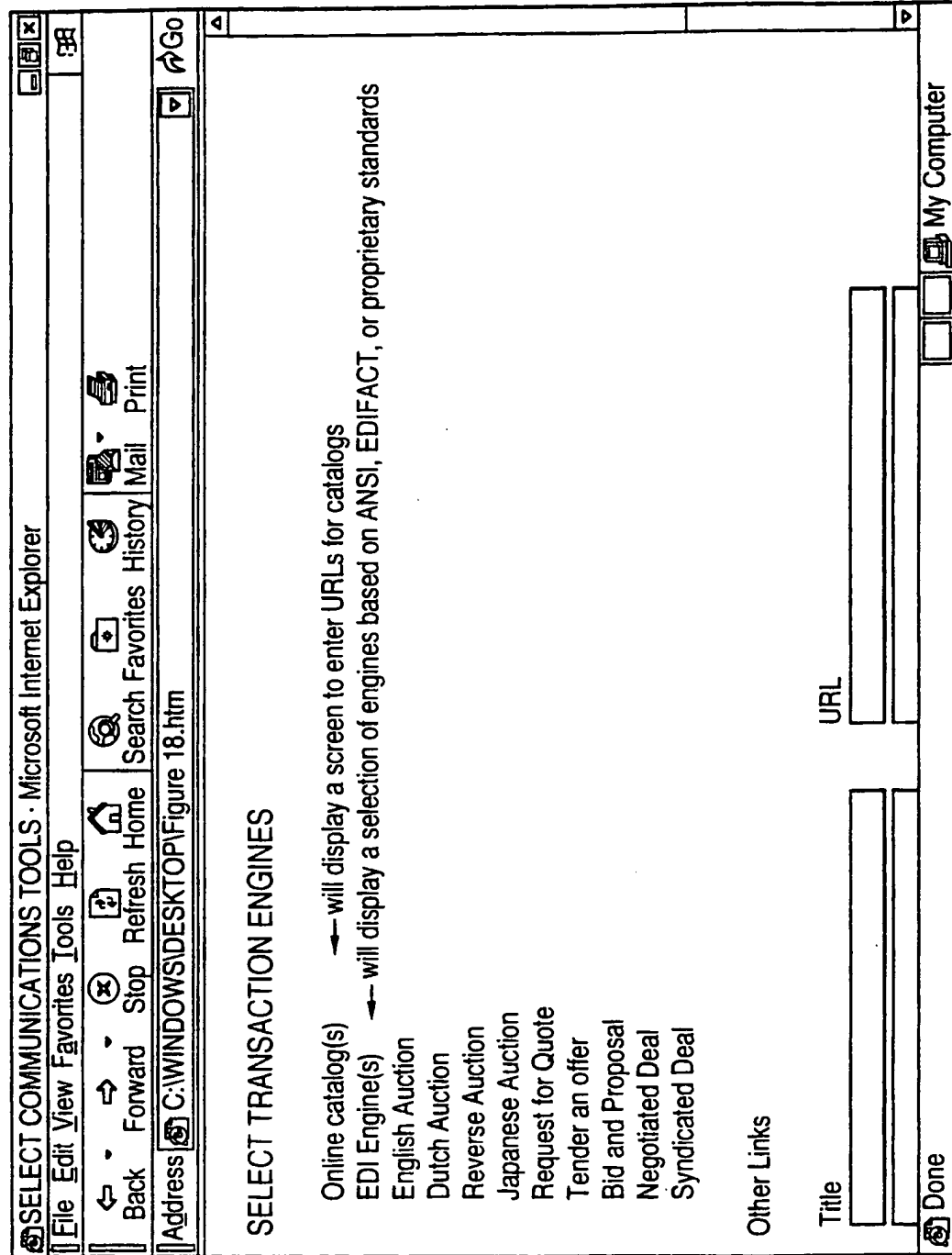


FIG. 18

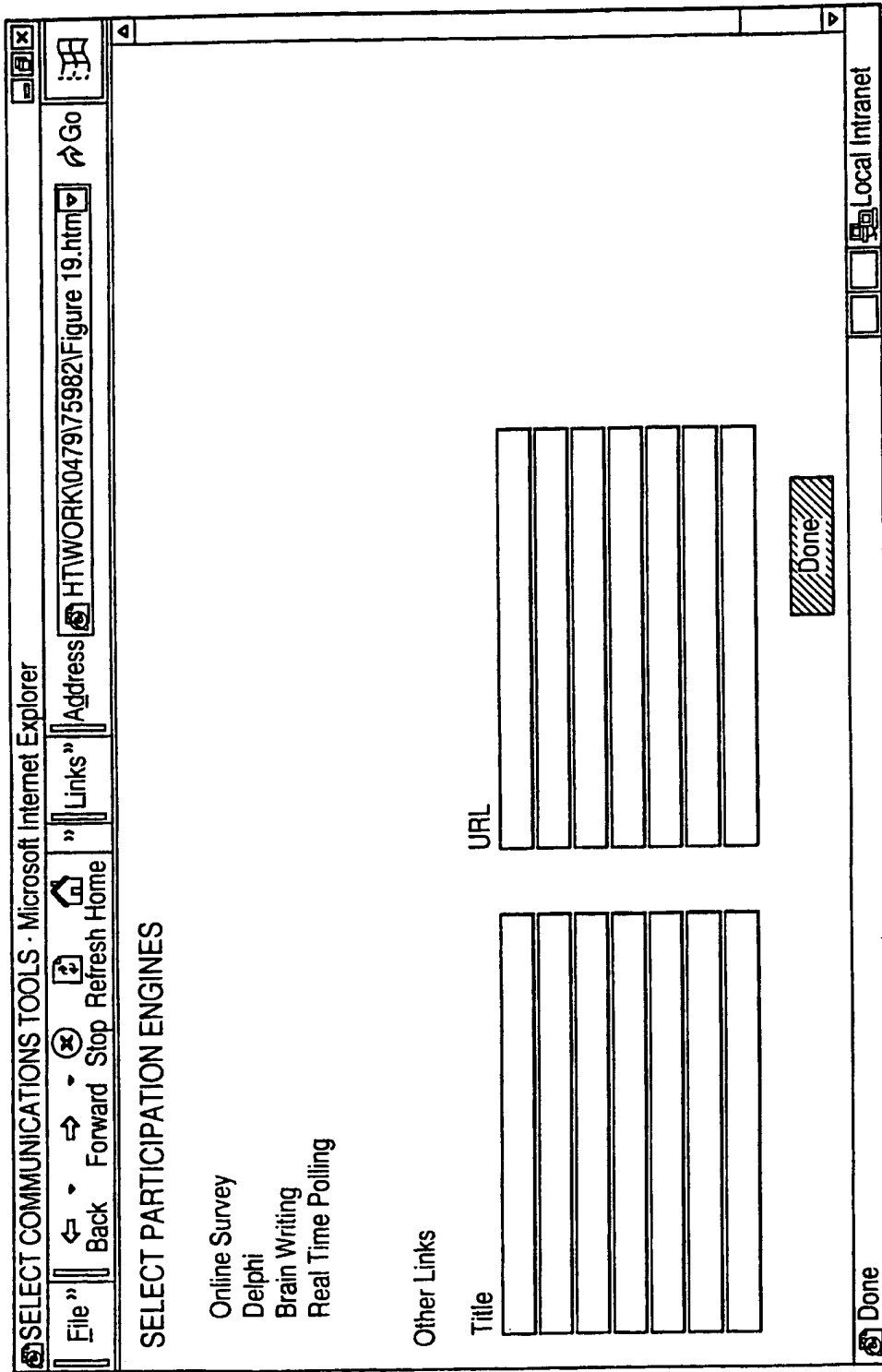


FIG. 19

SUBSTITUTE SHEET (RULE 26)

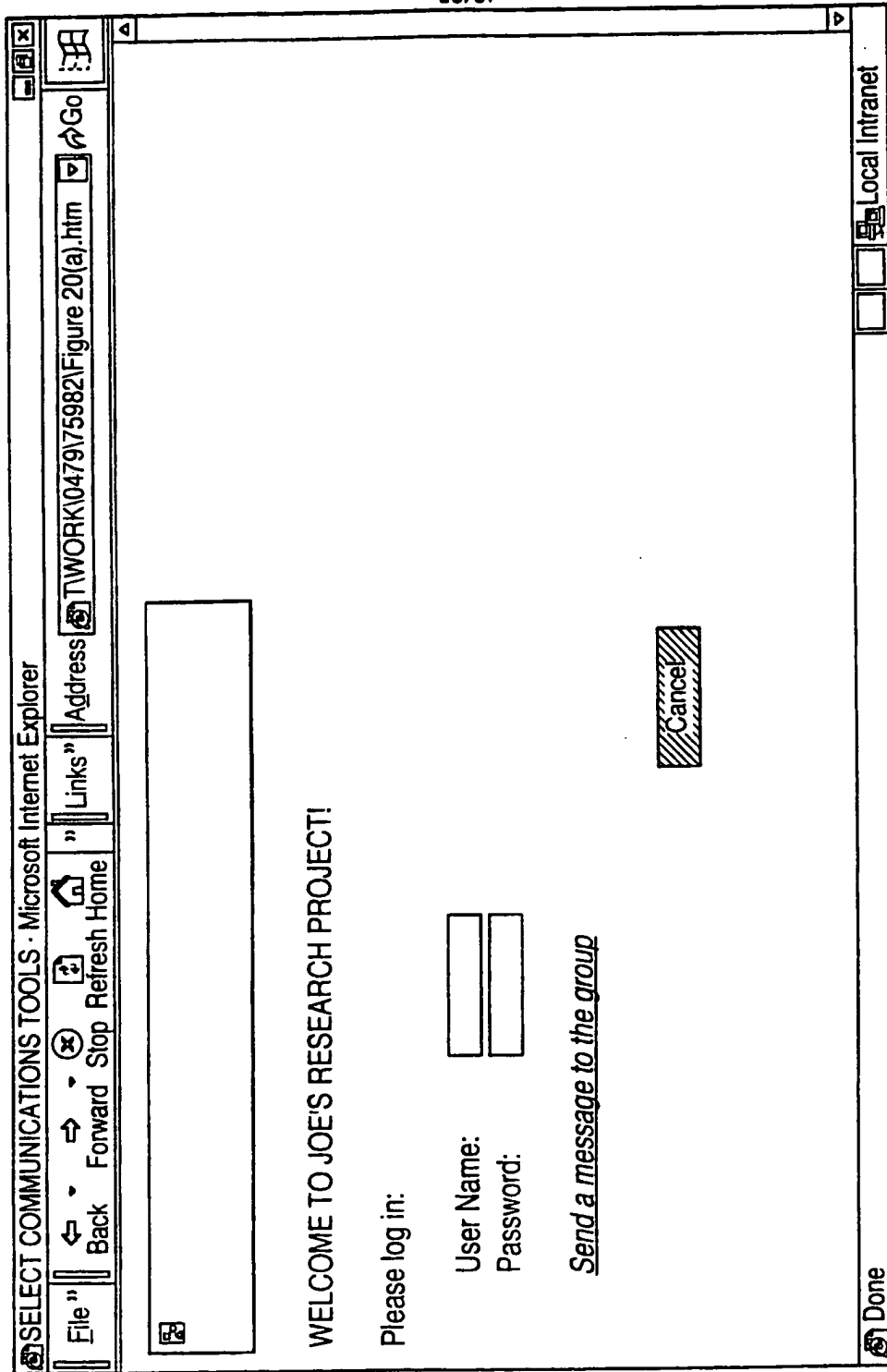


FIG. 20A

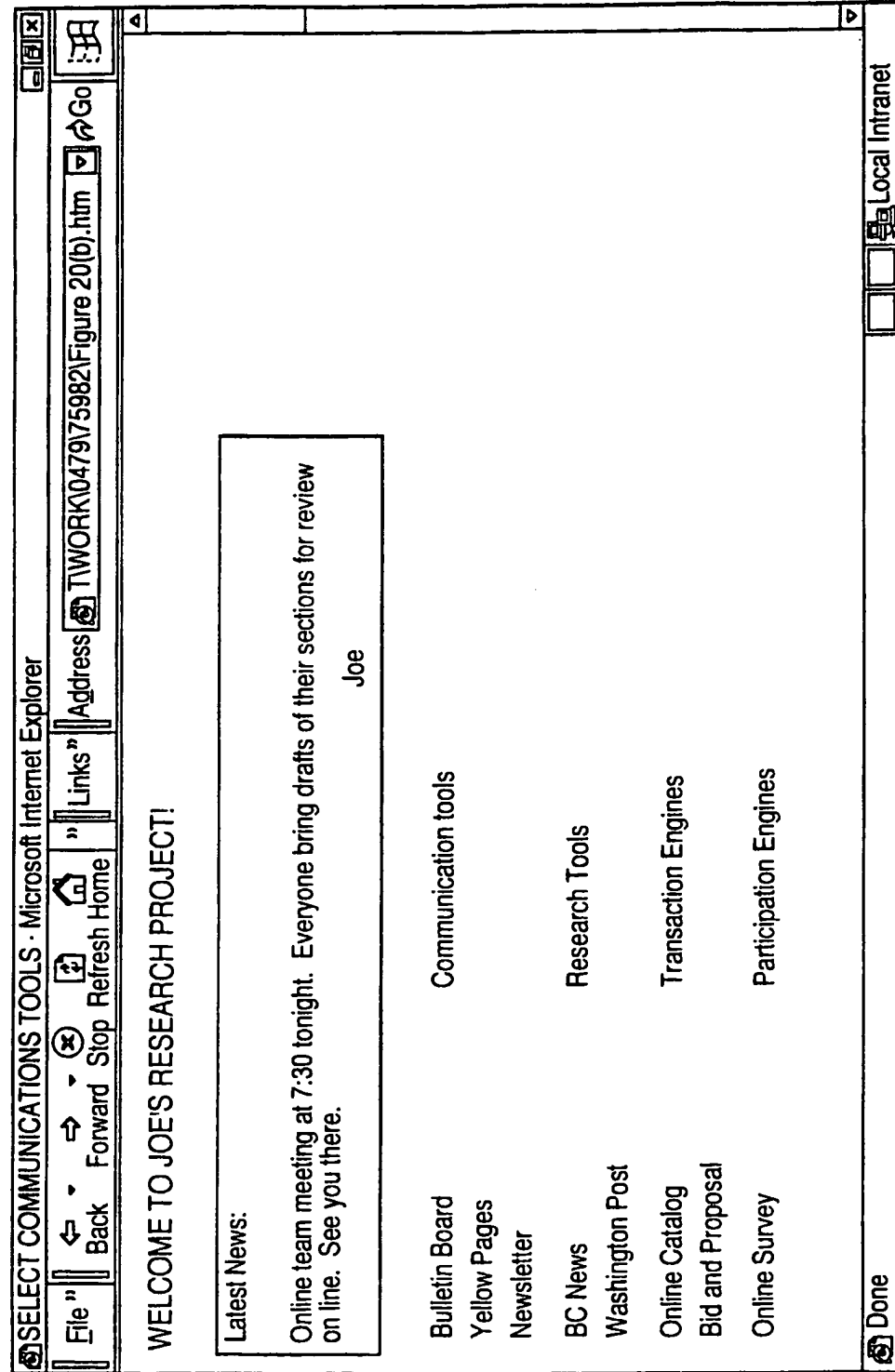


FIG. 20B

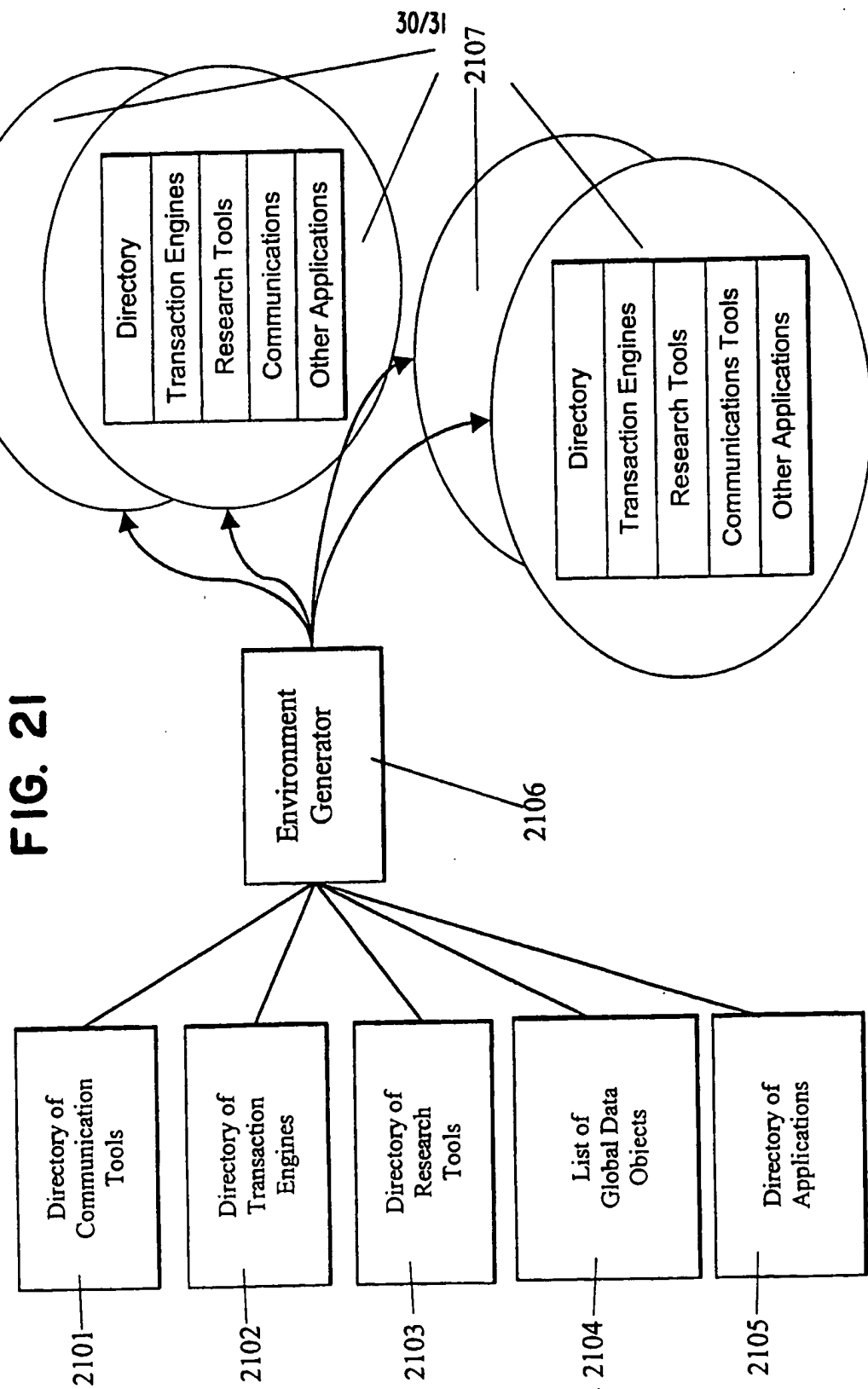
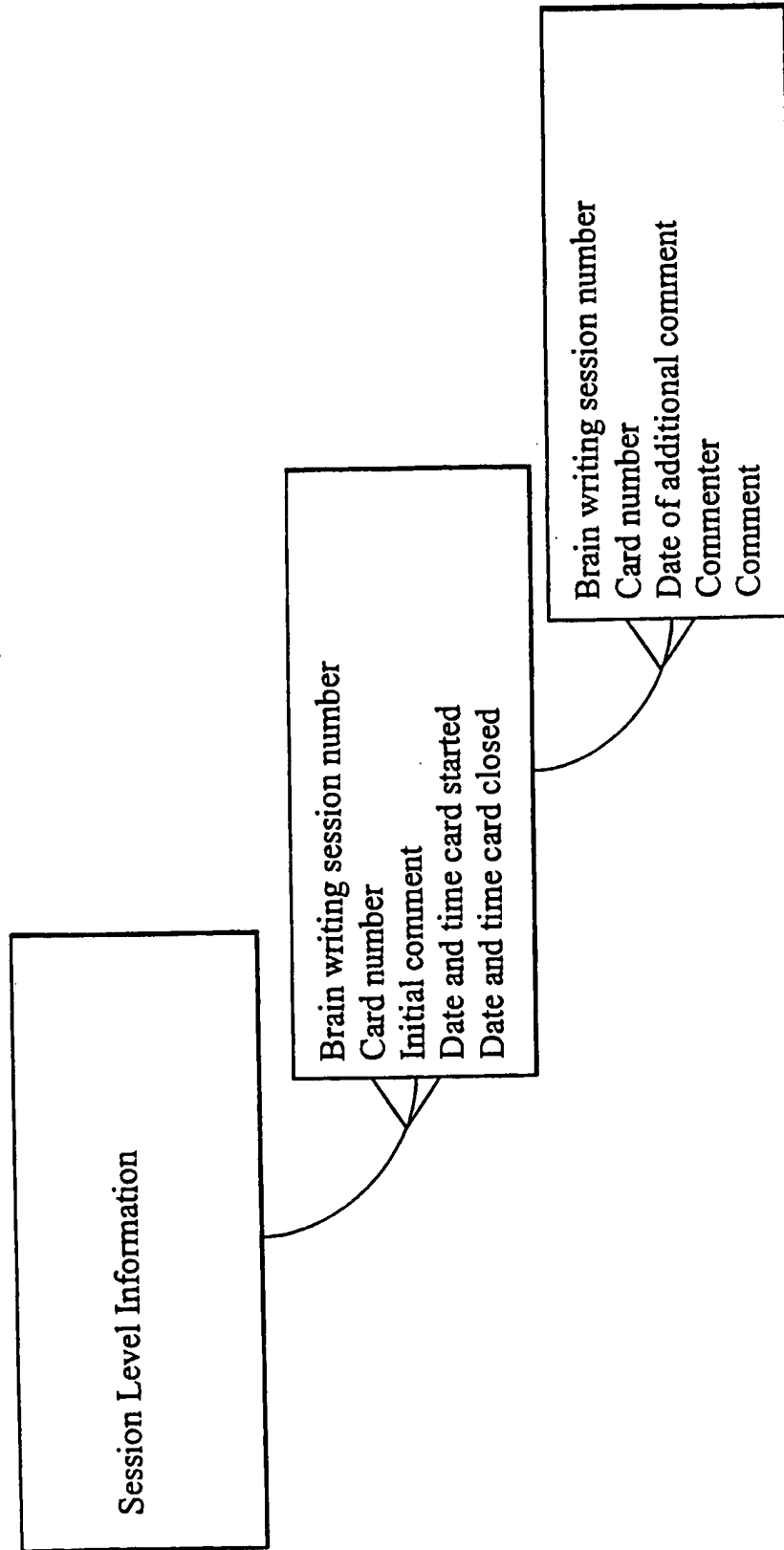


FIG. 22

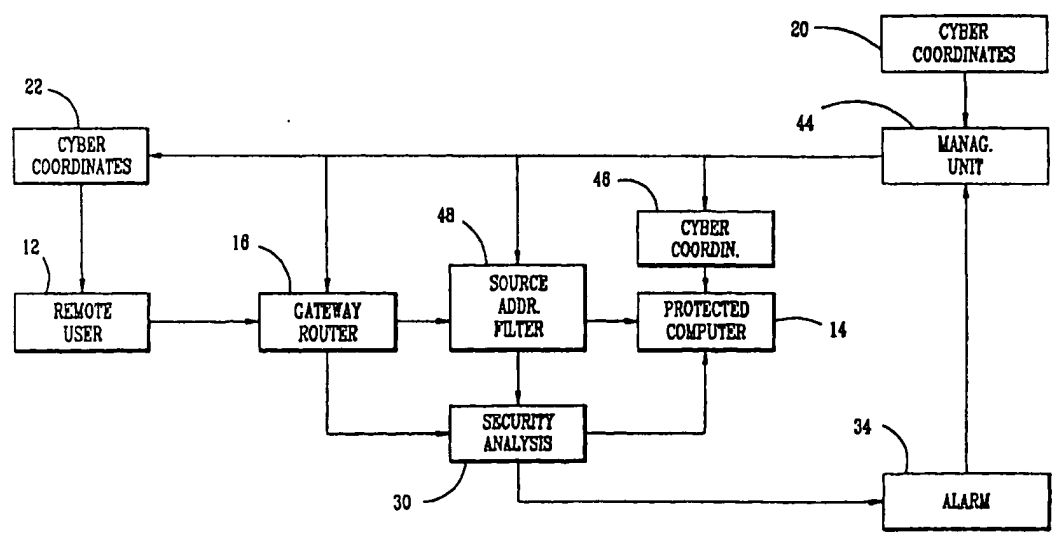




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification 7 : G06F 11/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 00/70458 (43) International Publication Date: 23 November 2000 (23.11.00)</p>
<p>(21) International Application Number: PCT/US00/08219 (22) International Filing Date: 15 May 2000 (15.05.00) (30) Priority Data: 60/134,547 17 May 1999 (17.05.99) US (71) Applicant: COMSEC CORPORATION [US/US]; 10217 Cedar Pond Drive, Vienna, VA 22182 (US). (72) Inventor: SHEYMOV, Victor, I.; 10217 Cedar Pond Drive, Vienna, VA 22182 (US). (74) Agent: SIXBEY, Daniel, W.; Nixon Peabody LLP, Suite 800, 8180 Greensboro Drive, McLean, VA 22102 (US).</p>	<p>(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report.</i></p>	

(54) Title: METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM



(57) Abstract

The intrusion protection method and system for a communication network provides address agility wherein the cyber coordinates of a target host (14) are changed both on a determined time schedule and when an intrusion attempt is detected. The system includes a management unit (18) which generates a random sequence of cyber coordinates and maintains a series of tables containing the current and next set of cyber coordinates. These cyber coordinates are distributed to authorized users (12) under an encryption process to prevent unauthorized access.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD OF COMMUNICATIONS AND
COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND
INTRUSION ATTEMPT DETECTION SYSTEM

5 This application is a continuation-in-part application of U.S. Serial No. 60/134,547
filed May 17, 1999.

Background Art

10 Historically, every technology begins its evolution focusing mainly on performance
parameters, and only at a certain developmental stage does it address the security aspects of
its applications. Computer and communications networks follow this pattern in a classic
way. For instance, first priorities in development of the Internet were reliability,
survivability, optimization of the use of communications channels, and maximization of their
15 speed and capacity. With a notable exception of some government systems, communications
security was not an early high priority, if at all. Indeed, with a relatively low number of
users at initial stages of Internet development, as well as with their exclusive nature,
problems of potential cyber attacks would have been almost unnatural to address,
considering the magnitude of other technical and organizational problems to overcome at
20 that time. Furthermore, one of the ideas of the Internet was "democratization" of
communications channels and of access to information, which is almost contradictory to the
concept of security. Now we are faced with a situation, which requires adequate levels of
security in communications while preserving already achieved "democratization" of
communications channels and access to information.

25 All the initial objectives of the original developers of the Internet were achieved with
results spectacular enough to almost certainly surpass their expectations. One of the most
remarkable results of the Internet development to date is the mentioned "democratization".
However in its unguarded way "democratization" apparently is either premature to a certain
percentage of the Internet users, or contrary to human nature, or both. The fact remains that
30 this very percentage of users presents a serious threat to the integrity of national critical
infrastructure, to privacy of information, and to further advance of commerce by utilization

of the Internet capabilities. At this stage it seems crucial to address security issues but, as usual, it is desirable to be done within already existing structures and technological conventions.

Existing communications protocols, while streamlining communications, still lack
5 underlying entropy sufficient for security purposes. One way to increase entropy, of course, is encryption as illustrated by U.S. Patent No. 5,742,666 to Finley. Here each node in the Internet encrypts the destination address with a code which only the next node can unscramble.

Encryption alone has not proven to be a viable security solution for many
10 communications applications. Even within its core purpose, encryption still retains certain security problems, including distribution and safeguarding of the keys. Besides, encryption represents a "ballast", substantially reducing information processing speed and transfer time. These factors discourage its use in many borderline cases.

Another way is the use of the passwords. This method has been sufficient against
15 humans, but it is clearly not working against computers. Any security success of the password-based security is temporary at best. Rapid advances in computing power make even the most sophisticated password arrangement a short-term solution.

Recent studies clearly indicate that the firewall technology, as illustrated by U.S.
Patent No. 5,898,830 to Wesinger et al., also does not provide a sufficient long-term solution
20 to the security problem. While useful to some extent, it cannot alone withstand the modern levels of intrusion cyber attacks.

On the top of everything else, none of the existing security methods, including
encryption, provides protection against denial of service attacks. Protection against denial
of service attacks has become a critical aspect of communication system security. All
25 existing log-on security systems, including those using encryption, are practically defenseless against such attacks. Given a malicious intent of a potential attacker, it is reasonable to assume that, even having failed with an intrusion attempt, the attacker is still capable of doing harm by disabling the system with a denial of service attack. Since existing systems by definition have to deal with every log-on attempt, legitimate or not, it is certain
30 that these systems cannot defend themselves against a denial of service attack.

The deficiencies of existing security methods for protecting communications systems leads to the conclusion that a new generation of cyber protection technology is needed to achieve acceptable levels of security in network communications.

5 Summary of the Invention

It is a primary object of the present invention to provide a novel and improved method of communications, and a novel and improved communication network intrusion protection method and systems and novel and improved intrusion attempt detection method and systems, adapted for use with a wide variety of communication networks including
10 Internet based computers, corporate and organizational computer networks (LANs), e-commerce systems, wireless computer communications networks, telephone dial-up systems, wireless dial-up systems, wireless telephone and computer communications systems, cellular and satellite telephone systems, mobile telephone and mobile communications systems,
15 cable based systems and computer databases, as well as protection of network nodes such as routers, switches, gateways, bridges, and frame relays.

Another object of the present invention is to provide a novel and improved communication network intrusion protection method and system which provides address agility combined with a limited allowable number of log-on attempts.

20 Yet another object of the present invention is to provide a novel and improved intrusion protection method for a wide variety of communication and other devices which may be accessed by a number, address code, and/or access code. This number, address code, and/or access code is periodically changed and the new number, address code, or access code is provided only to authorized users. The new number, address code, or access code may be
25 provided to a computer or a device for the authorized user and not be accessible to others. This identifier causes the user's computer to transmit the otherwise unknown and inaccessible number, address code, and/or access code.

A still further object of the present invention is to provide a novel and improved communication network intrusion protection method and system wherein a plurality of
30 different cyber coordinates must be correctly provided before access is granted to a protected communications unit or a particular piece of information. If all or some cyber coordinates

are not correctly provided, access is denied, an alarm situation is instigated and the affected cyber coordinates may be instantly changed.

For the purposes of this invention cyber coordinates are defined as a set of statements determining location of an object (such as a computer) or a piece of information (such as a computer file) in cyber space. Cyber coordinates include but are not limited to private or public protocol network addresses such as an IP address in the Internet, a computer port number or designator, a computer or database directory, a file name or designator, a telephone number , an access number and/or code, etc.

These and other objects of the present invention are achieved by providing a communication network intrusion protection method and system where a potential intruder must first guess where a target computer such as a host workstation is in cyber space and to predict where the target computer such as a workstation will next be located in cyber space. This is achieved by changing a cyber coordinate (the address) or a plurality of cyber coordinates for the computers such as workstations on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the cyber coordinates are changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of addresses. These addresses are distributed to authorized parties, usually with use of an encryption process.

The present invention further provides for a piece of information, a computer or a database intrusion protection method and system where a potential intruder must first guess where a target piece of information such as a computer file or a directory is in cyber space and to predict where the target piece of information will be next in cyber space. This is achieved by changing a cyber coordinate or a plurality of cyber coordinates for the piece of information on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the coordinates changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of cyber coordinates. These coordinates are distributed to authorized parties, usually by means

of an encryption process.

The intrusion attempt detection methods and systems are provided to the protected devices and pieces of information as described above by means of categorizing a log-on attempt when all or some of the correct cyber coordinates are not present as an intrusion attempt and by instigating an alarm situation.

Brief Description of the Drawings

Figure 1 is a block diagram of the communication network protection system of the present invention;

Figure 2 is a flow diagram showing the operation of the system of Figure 1;

Figure 3 is a block diagram of a second embodiment of the communication network protection system of the present invention;

Figure 4 is a flow diagram showing the operation of the system of Figure 3;

Figure 5 is a block diagram of a third embodiment of the communication network protection system of the present invention;

Figure 6 is a flow diagram showing the operation of the system of Figure 5; and

Figure 7 is a block diagram of a fourth embodiment of the communication network protection system of the present invention.

Description of the Preferred Embodiments

Existing communications systems use fixed coordinates in cyber space for the communications source and communications receiver. Commonly accepted terminology for the Internet refers to these cyber coordinates as source and destination IP addresses. For

purposes of an unauthorized intrusion into these communication systems, the situation of a cyber attack might be described in military terms as shooting at a stationary target positioned at known coordinates in cyber space. Obviously, a moving target is more secure than the stationary one, and a moving target with coordinates unknown to the intruder is more secure yet. The method of the present invention takes advantage of the cyber space environment and the fact that the correlation between the physical coordinates of computers or other communication devices and their cyber coordinates is insignificant.

While it is difficult to change the physical coordinates of computers or other communications devices, their cyber coordinates (cyber addresses) can be changed much easier, and in accordance with the present invention, may be variable and changing over time. In addition to varying the cyber coordinates over time, the cyber coordinates can immediately be changed when an attempted intrusion is sensed. Furthermore, making the current cyber coordinates available to only authorized parties makes a computer or other communications device a moving target with cyber coordinates unknown to potential attackers. In effect, this method creates a device which perpetually moves in cyber space.

Considering first the method of the present invention as applied to computers and computer networks, the computer's current cyber address may serve also as its initial log-on password with a difference that this initial log-on password is variable. A user, however, has to deal only with a computer's permanent identifier, which is, effectively its assigned "name" within a corresponding network. Any permanent identifier system can be used, and an alphabetic "name" system seems to be reasonably user-friendly. One of such arrangements would call for using a computer's alphabetic Domain Name System, as a cyber address permanent identifier, while subjecting its numeric, or any other cyber address to a periodic change with regular or irregular intervals. This separation will make the security system transparent to the user, who will have to deal only with the alphabetic addresses. In effect, the user's computer would contain an "address book" where the alphabetic addresses are permanent, and the corresponding variable addresses are more complex and periodically updated by a network's management. While a user is working with other members of the network on the name or the alphabetic address basis, the computer conducts communications based on the corresponding variable numeric or other addresses assigned for that particular time.

A variable address system can relatively easily be made to contain virtually any level of entropy, and certainly enough entropy to defy most sophisticated attacks. Obviously, the level of protection is directly related to the level of entropy contained in the variable address system and to the frequency of the cyber address change.

5 This scenario places a potential attacker in a very difficult situation when he has to find the target before launching an attack. If a restriction on a number of allowable log-on tries is implemented, it becomes more difficult for an attacker to find the target than to actually attack it. This task of locating the target can be made difficult if a network's cyber address system contains sufficient entropy. This difficulty is greatly increased if the security
10 system also limits the number of allowable log-on tries, significantly raising the entropy density.

For the purpose of this invention, entropy density is defined as entropy per one attempt to guess a value of a random variable.

Figure 1 illustrates a simple computer intrusion protection system 10 which operates
15 in accordance with the method of the present invention. Here, a remote user's computer 12 is connected to a protected computer 14 by a gateway router or bridge 16. A management system 18 periodically changes the address for the computer 14 by providing a new address from a cyber address book 20 which stores a plurality of cyber addresses. Each new cyber address is provided by the management system 18 to the router 16 and to a user computer
20 address book 22. The address book 22 contains both the alphabetic destination address for the computer 14 which is available to the user and the variable numeric cyber address which is not available to the user. When the user wants to transmit a packet of information with the alphabetic address for the computer 14, this alphabetic address is automatically substituted for the current numerical cyber address and used in the packet.

25 With the reference to Figures 1 and 2, when a packet is received by the gateway router or bridge 16 as indicated at 24, the cyber address is checked by the gateway router or bridge at 26, and if the destination address is correct, the packet is passed at 28 to the computer 14. If the destination address is not correct, the packet is directed to a security analysis section 30 which, at 32 determines if the packet is retransmitted with a correct
30 address within a limited number of log-in attempts. If this occurs, the security analysis section transmits the packet to the computer 14 at 28. However, if no correct address is

received within the allowed limited number of log-in attempts, the packet is not transmitted to the computer 14 and the security analysis section activates an alarm section 34 at 36 which in turn causes the management section to immediately operate at 38 to change the cyber address.

5 Sophisticated cyber attacks often include intrusion through computer ports other than the port intended for a client log-on. If a system principally described in connection with Figures 1 and 2 is implemented, the port vulnerability still represents an opening for an attack from within the network, that is if an attacker has even a low-level authorized access to a particular computer and thus knows its current variable address.

10 Computer ports can be protected in a way similar to protection of the computer itself. In this case port assignment for the computer becomes variable and is changed periodically in a manner similar to that described in connection with Figures 1 and 2. Then, a current assignment of a particular port is communicated only to appropriate parties and is not known to others. At the same time, similarly to methods described, a computer user would deal
15 with permanent port assignments, which would serve as the ports' permanent "names".

 This arrangement in itself may not be sufficient, however, to reliably protect against a port attack using substantial computing power because of a possible insufficient entropy density. Such a protection can be achieved by implementing an internal computer "port
20 gateway router or bridge 16 serves for computer destination addresses.

 With reference to Figures 3 and 4 wherein like reference numerals are used for components and operations which are the same as those previously described in connection with Figures 1 and 2, a port router 40 is provided prior to the protected computer 14, and this
25 port router is provided with a port number or designator by the management unit 18. This port number or designator is also provided to the user address book 22 and will be changed when the cyber address is changed, or separately. Thus, with reference to Figure 4, once the cyber address has been cleared at 26, the port number or designator is examined at 42. If the port number is also correct, the data packet will be passed to the computer 14 at 28. If the port number is initially incorrect, the packet is directed to the security analysis section 30
30 which at 32 determines if the packet is retransmitted with the correct port number within the limited number of log-in attempts.

The port protection feature can be used independently of other features of the system. It can effectively protect nodes of the infrastructure such as routers, gateways, bridges, and frame relays from unauthorized access. This can protect systems from an attacker staging a cyber attack from such nodes.

5 The method and system of the present invention may be adapted to provide security for both Internet based computer networks and private computer networks such as LANs.

Internet structure allows the creation of an Internet based Private Cyber Network (PCN) among a number of Internet-connected computers. The main concern for using the Internet for this purpose as an alternative to the actual private networks with dedicated
10 communication channels is security of Internet-based networks.

The present invention facilitates establishment of adequate and controllable level of security for the PCNs. Furthermore, this new technology provides means for flexible structure of a PCN, allowing easy and practically instant changes in its membership. Furthermore, it allows preservation of adequate security in an environment where a computer
15 could be a member of multiple PCNs with different security requirements. Utilizing the described concept, a protected computer becomes a "moving target" for the potential intruders where its cyber coordinates are periodically changed and the new coordinates are communicated on a "need to know" basis only to the other members of the PCN authorized to access this computer along with appropriate routers and gateways. This change of cyber
20 coordinates can be performed either by previous arrangement or by communicating future addresses to the authorized members prior to the change. Feasible frequency of such a change can range from a low extreme of a stationary system changing cyber coordinates only upon detection of a cyber attack to an extremely high frequency such as with every packet. The future coordinates can be transmitted either encrypted or unencrypted. Furthermore,
25 each change of position of each PCN member can be made random in terms of both its current cyber coordinates and the time of the coordinates change. These parameters of a protected PCN member's cyber moves are known only to the PCN management, other PCN members with authorization to communicate with this particular member, and appropriate gateways and routers. PCN management would implement and coordinate periodic cyber
30 coordinates changes for all members of the PCN. While the PCN management is the logical party to make all the notification of the cyber coordinates changes, in certain instances it

could be advantageous to shift a part of this task to a PCN member computer itself. With certain limitations, the routers and gateways with the "need to know" the current address of the protected computer are located in cyber space in the general vicinity of the protected computer. In such instances the protected computer could be in a better position to make the mentioned notifications of nearby routers and gateways.

The address changes could be done simultaneously for all the members of the PCN, or separately, particularly if security requirements for the members substantially differ. The latter method is advantageous, for instance, if some of the computers within the PCN are much more likely than others to be targeted by potential intruders. A retail banking PCN could be an example of such an arrangement where the bank's computer is much more likely to be attacked than a customer's computer. It should be noted that, while in certain cases some members of the PCN may not require any protection at all, it still is prudent to provide it as long as the computer belongs to a protected PCN. The correct "signature" of the current "return address" would serve as additional authenticity verification. In the above example of the retail banking, while many customers' computers may not require any protection, assigning variable addresses to them would serve as an additional assurance to the bank that every log-on is authorized. In fact, this system automatically provides two-tier security. In order to reach a protected computer, the client computer has to know the server computer current cyber address in the first place. Then, even if a potential intruder against odds "hits" the correct current address the information packet is screened for the correct "signature" or return address. If that signature does not belong to the list of the PCN's current addresses, the packet is rejected. In high security instances this should trigger an unscheduled address change of the protected computer.

With the reference to Figures 5 and 6 which illustrate this two-tier security system, a network management unit 44 provides different unique cyber coordinates to the address books for each computer in the system (two computers 12 and 14 with address books 22 and 46 respectively being shown). Now when the computer 12 sends a data packet to the computer 14, the gateway router or bridge 16, first checks for the correct current destination address for the computer 14 at 26 in the manner previously described. If the destination address is correct, a source address sensor 48 checks at 50 to determine if the correct source address (i.e. return address) for the computer 12 is also present. If both correct addresses are

present, the data packet is passed to the computer 14 at 28, but if the correct source address is not present, the data packet is passed to the security analysis section 30 where at 32 where it is determined if a correct source address is received within the acceptable number of log-on tries. If the correct return address is not received, an alarm situation is activated at 36 and the network management system operates at 38 to change the cyber address of the computer 14

In addition to the penetration (hacking) detection and protection, the system above provides real-time detection of a cyber attack and protection against "flooding" denial of service attacks. A gateway router or bridge 16 filters all the incorrectly addressed packets thus protecting against "flooding". Further yet, since the "address book" of the protected network contains only trusted destinations, this system also protects against instructive viruses or worms if such are present or introduced into the network. For the purpose of this invention, an instructive virus or worm is defined as a foreign unit of software introduced into a computer system so it sends certain computer data to otherwise unauthorized parties outside of the system.

Elements of the system described above are: a gateway router or bridge 16, a computer protection unit, and a management unit. A gateway router or bridge represents an element of collective defense for the network, while the source address filter and the "port router" and filter represent a unit of individual defense for a member computer. This individual defense unit (server unit) can be implemented either as a standalone computer, as a card in the protected computer, as software in the protected computer, or imbedded into the protected computer operating system. For further improvement of the overall security, port assignments can be generated autonomously from the management unit thus creating a "two keys" system in a cryptographic sense. This would allow for security to still be in place even if a security breach happened at the security management level.

The method and system of the present invention minimize human involvement in the system. The system can be configured in such a way that computer users deal only with simple identifiers or names permanently assigned to every computer in the network. All the real (current) cyber coordinates can be stored separately and be inaccessible to the user, and could be available to the appropriate computers only. This approach both enhances security and makes this security system transparent to the user. The user deals only with the simple

5 alphabetic side of the "address book", and is not bothered with the inner workings of the security system. A telephone equivalent of this configuration is an electronic white pages residing in a computerized telephone set, which is automatically updated by the telephone company. The user just has to find a name, and push the "connect" button while the telephone set does the rest of the task.

10 A numeric cyber address system, based on the Internet host number could be relatively easily utilized for the discussed security purposes, however a limitation exists for this address system in its current form represented by the IPv.4 protocol. This limitation is posed by the fact that the address is represented by a 32-bit number. 32-bit format does not contain sufficient entropy in the address system to enable establishment of adequate security. This is a particularly serious limitation in regard to securing an entire network. The availability of the network numbers are limited to the extent that not only entropy, but a simple permanently assigned number is becoming more and more difficult to obtain with the rapid expansion of the Internet.

15 If this address system is to be used for the security purposes, than the format of the host number should be adequately expanded to create sufficient size of the address numbers field in the system. If this is done, than the corresponding address in the Domain Name System (DNS) could be conveniently used as permanent identifier for a particular computer and the Internet host number would be variable, creating a moving regime of a protected computer. Currently being implemented IPv.6 (IPNG) protocol solves this problem by providing sufficient entropy.

20 Another way to achieve the same goal is to use the DNS address as a variable for security purposes. This way, the traditional Internet DNS address system would not be affected and no change in format is required. The relevant part of the protected computer's DNS address would become a variable, utilizing more characters than the alphabet, with a very large number of variations, also creating sufficient level of entropy.

25 Yet another way to implement the same method is to utilize the geographic zone-based system. While its utilization is somewhat similar to the DNS system, it offers some practical advantages for security use. Naturally, when a computer is protected by a security system, it is still essential to preserve the communication redundancy of the Internet communications. However, the redundancy may suffer if only a limited number of the

30

routers and gateways are informed of the protected computer current cyber address. This effect could be particularly important with the members of a particular protected network vastly remote in geographic terms. The necessary notification of a large number of the routers and gateways can also become problematic, not only technically, but also because it can decrease the level of security. In this sense a geographic zone-based system offers advantages since the variable part of the computer's cyber address could be made to involve only certain geographic locale while initial routing of the information packet could be done by the traditional method. After the packet has been moved to the general vicinity of the addressee computer, it would get into the area of the "informed" routers and gateways. This scheme would simplify the notification process of the routers as well as improve security by limiting the number of the "need to know" parties. It is important to recognize that, after the "general" part of the cyber address caused the information packet to arrive in a cyber vicinity of the addressee, virtually any, even private, address system can be used for the rest of the delivery. This would further increase the level of underlying entropy in the system.

While certain specific address systems have been discussed, it is an important quality of the present invention that it can be implemented with virtually any address system.

Corporate and organizational computer networks such as LANs or, at least those in closed configurations, do not possess as much vulnerability to cyber attacks as Internet-based networks. However, even in these cases, their remote access security is a subject of concern. This is especially visible when a private network (PN) contains information of different levels of confidentiality with access restricted to appropriate parties. In other words, along with other generally accessible organizational information, an organizational PN can contain information restricted to certain limited groups. Enforcement of these restrictions requires a remote access security system. Usually these security systems employ a password-based scheme of one type or another and, perhaps, a firewall. However, reliance on passwords may not be entirely justified since the passwords can be lost or stolen, giving a malicious insider with a low access level a reasonable chance of access to information intended only for higher levels of access. Furthermore, in some cases use of cracking techniques from such a position is not entirely out of the question. Such an occurrence can relatively easily defeat both the password and the firewall. This would prevent a LAN from a cyber attack launched from within the network.

The present invention provides adequate security to such PCNs without reliance on the passwords and to limit access to only appropriate computers. Then, the task of overall information access security practically would be narrowed down to control of physical access to a particular computer, usually a less complicated feat.

5 Similarly to the systems described for Internet-based networks, a "closed" LAN as well as an Internet-based LAN can be protected by implementation of periodic changes of the members' network addresses and communicating those changes to the appropriate parties. This way, the lowest access level computers would have the lowest rate of address change. The rate of the address change would increase with the level of access. This system
10 would ensure that all the PCN computers with legitimate access to a particular computer within the PCN would be informed of its location. Furthermore, it will ensure that the current location of a computer with restricted information would be unknown to the parties without the legitimate access clearance. For instance, a superior's computer would be able to access his subordinate's computer but not vice versa.

15 Also similarly to the systems described for the PCNs, a PCN computer would contain an "address book" where the user can see and use only the permanent side of it with identifiers of all computers accessible to him while the actual communication functions are performed by the computer using the variable side of the "address book" periodically updated by the PN management. To further enhance security, in addition to the computer
20 address system management, the PCN Administrator can implement an automatic security monitoring system where all wrongly addressed log-on attempts would be registered and analyzed for security purposes.

Thus the method and system of the present invention would allow reliable protection against unauthorized remote access to information from within a PN while providing a great
25 deal of flexibility, where the granted access can be revised easily and quickly.

A greatly enhanced intrusion protection system and method can be achieved by combining the operating systems of Figures 1-6. Now an arriving data packet would first be screened by a gateway router or a similar device for a correct destination address. If the destination address is correct, the packet is passed for further processing. If the destination
30 address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The packet with correct destination address is then screened for a correct source address. If the source address is correct, the packet is passed to the receiver computer. If the source address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

5 Then, the packet with a correct destination address and a correct source address is screened for a correct allowed port coordinate such as port number. If the port coordinate is correct, the packet is passed for further processing. If the port coordinate is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

10 Finally, the packet with a correct destination and source addresses and a correct port designator is screened for data integrity by application of authentication check such as a checksum. If the authentication check is passed, the packet is passed to the addressee computer. If the authentication check is failed, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

15 The security managing unit analyses all the alarms and makes decisions on necessary unscheduled changes of addresses for appropriate network servers. Also, it can notify law enforcement and pass appropriate data on to it.

Figure 7 illustrates an enhanced computer intrusion protection system indicated generally at 52 for one or more network computers 54. A gateway router or a bridge 58 includes a destination address filter 60 which receives data packets which pass in through a load distribution switch 62. A non-interrogatable network address book 64 stores current network server addresses for the destination address filter 60, and the destination address filter checks each data packet to determine if a legitimate destination address is present.

25 Packets with legitimate destination addresses are forwarded to a source address filter 66, while packets with illegitimate destination addresses are sent to a security analysis section 68 in a management unit 70.

30 When a preset traffic load level is reached indicating that an attempt at flooding is being made, the destination address filter causes the load distribution switch 62 to distribute traffic to one or more parallel gateway routers or bridges which collectively forward legitimate traffic and dump the flooding traffic. An alternative arrangement would call for the load distribution function to be done irrespective of the load, utilizing all the parallel

gateways all the time. A source address table 74 stores accessible server's designators and corresponding current addresses for all system servers which may legitimately have access to the computer or computers 54. These addresses are accessed by the source address filter which determines whether or not an incoming data packet with the proper destination address originates from a source with a legitimate source address entered in the source address table 74. If the source address is determined to be legitimate, the data packet is passed to a port address filter 76. Data packets with an illegitimate source address are directed to the security analysis section 68. Alternatively, source address screening can be done at the gateway router or bridge 58 first prior to port filter 76.

A port protection table 78 includes the current port assignments for the computer or computers 54, and these port assignments are accessed by the port designator filter 76 which then determines if an incoming data packet contains legitimate port designation. If it does, it is passed to an actual address translator 80 which forwards the data packet to the specific computer or computers 54 which are to receive the packet. If an illegitimate port address is found by the port address filter 76, the data packet is transmitted to the security analysis section 68.

The management unit 70 is under the control of a security administrator 82. A network membership master file 84 stores a master list of legitimate server's designators along with respective authorized access lists and corresponding current cyber coordinates. The security administrator can update the master list by adding or removing authorized access for every protected computer. An access authorization unit 86 distributes the upgraded relevant portions of the master lists to the address books of the respective authorized servers.

A random character generator 88 generates random characters for use in forming current port designators, and provides these characters to a port designator forming block 90. This port designator forming block forms the next set of network current port designators in conjunction with the master list and these are incorporated for transmission by a port table block 92. Alternatively, port designators can be formed in the computer unit instead of the management unit.

Similarly, a random character generator 94 generates random characters for use in forming current server addresses, and provides these characters to a server address forming

block 96. This server address forming block forms the next set of current network server addresses, and an address table 98 assigns addresses to servers designated on the master list.

A coordinator/dispatcher block 100 coordinates scheduled move of network servers to their next current addresses, provides the next set of network addresses for appropriate servers and routers and coordinates unscheduled changes of addresses on command from the security analysis unit 68. The coordinator/dispatcher block 100 may be connected to an encode/decode block 102 which decodes received address book upgrades from input 104 and encodes new port and server destination addresses to be sent to authorized servers in the system over output 106. Where encoding of new cyber coordinates is used, each authorized computer in the network will have a similar encoding/decoding unit.

The security analysis unit 68 analyses received illegitimate data packets and detects attack attempts. If needed, the security analysis unit orders the coordinator/dispatcher block 100 to provide an unscheduled address change and diverts the attack data packets to an investigation unit 108. This investigation unit simulates the target server keeping a dialog alive with the attacker to permit security personnel to engage and follow the progress of the attacker while tracing the origin of the attack.

Providing security against intrusion for e-commerce systems presents a unique problem, for an important peculiarity of an e-commerce system is that its address must be publicly known. This aspect represents a contradiction to the requirement of the address being known to authorized parties only. However, the only information intended for the general public usually relates to a company catalog and similar material. The rest of the information on a merchant's network is usually considered private and thus should be protected. Using this distinction, a merchant's e-commerce site should be split into two parts: public and private. The public part is set up on a public "catalog" server with a fixed IP address and should contain only information intended for the general public. The rest of the corporate information should be placed in a separate network and protected as described in relation to Figures 1-7.

When a customer has completed shopping and made purchasing decisions concerning the terms and price of the sale, pertinent for the transaction, information is placed in a separate register. This register is periodically swept by a server handling financial transactions ("financial" server), which belongs to the protected corporate network. In fact,

the "catalog" server does not know the current address of the financial transactions server. Thus, even if an intruder penetrates the "catalog" server, the damage is limited to the contents of the catalog and the intruder cannot get an entry to the protected corporate network.

5 The financial server, having received pending transaction data, contacts the customer, offering a short-term temporary access for finalizing the transaction. In other words, the customer is allowed access just long enough to communicate pertinent financial data such as a credit card number and to receive a transaction confirmation at which point the session is terminated, the customer is diverted back to the catalog server and the financial server is
10 moved to a new cyber address thus making obtained knowledge of its location during the transaction obsolete.

Dial-up communications systems, in respect to their infrastructure channels susceptibility to transmission intercept by unrelated parties, can be separated into two broad categories: easily interceptable, such as cellular and satellite telephone systems and relatively
15 protected such as conventional land-line based telephone systems. Relatively protected systems such as conventional land-line based telephone systems can be protected in the following way. Phone numbers, assigned by a telephone company to a dial-up telephone-based private network serve as the members' computer addresses. As described previously, such a private network can be protected from unauthorized remote access by implementing
20 periodic changes in the addresses, i.e. telephone numbers assigned to the members for transmission by the network along with other designators such as access codes and communicating the changed numbers to the appropriate parties.

For the conventional land-line dial-up telephone systems, while the "last mile" connection remains constant, the assigned telephone number is periodically changed, making
25 the corresponding computer a moving target for a potential attacker. In this case the telephone company serves as the security system manager. It assigns the current variable telephone numbers to the members of a protected, private network, performs notification of all the appropriate parties, and changes the members' current numbers to a new set at an appropriate time. The telephone company switches naturally serve in the role of routers, and
30 thus they can be programmed to perform surveillance of the system, to detect potential intrusion attacks and to issue appropriate alarms.

Periodically changing the current assigned numbers creates system entropy for a potential intruder, making unauthorized access difficult. Obviously, the implementation of this security system is dependent on availability of sufficient vacant numbers at a particular facility of the telephone company. Furthermore, for a variety of practical reasons it is advisable to keep a just vacated number unassigned for a certain period of time. All this may require additional number capacity at the telephone company facility in order to enable it to provide remote access security to a larger number of personal networks while preserving a comfortable level of system entropy.

If the mentioned additional capacity is not available, or a still higher level of entropy is desired, it could be artificially increased by adding an access code to the assigned number. This would amount to adding virtual capacity to the system, and would make a combination of the phone number and access code an equivalent of a computer's telephone address. In effect, this would make a dialed number larger than the conventional format. This method makes a virtual number capacity practically unlimited and, since the process is handled by computers without human involvement, it should not put any additional burden on a user. With or without a virtual number capacity, utilization of this method allows the intrusion attempts to be easily identified by their wrong number and/or code. At the same time, implementation of this system might require some changes in dialing protocols as well as additional capabilities of the telephone switching equipment.

Entropy density can be increased by limiting the number of allowable connection attempts. Similarly to the method described previously, telephone company switching equipment can be made to perform a role of an outside security barrier for the private network. In this case wrongly addressed connection attempts should be analyzed in order to detect possible "sweeping". If such an attempt is detected, tracing the origin of the attempt and notifying the appropriate phone company should not present a problem even with the existing technology.

The simplest form of private network protection under the proposed method and system is when at a predetermined time all the members of a particular network are switched to the new "telephone book" of the network. However, in some cases required level of security for some members of the same private network could substantially differ, or they may face different levels of security risk. In such cases frequency of the phone number

change could be set individually with appropriate notification of the other members of the network. This differentiation enables the telephone company to offer differentiated levels of security protection to its customers even within the same private network.

5 A telephone company can also offer its customers protected voice private networks which would provide a higher level of privacy protection than the presently used "unlisted numbers." In this configuration the customers' telephone sets are equipped with a computerized dialing device with remotely upgradeable memory which would allow each member of a protected voice network to contain the network "telephone book" and that book is periodically updated by the telephone company.

10 The telephone company would periodically change the assigned telephone numbers of a protected network to a new set of current numbers. These new numbers would be communicated to the members of a protected voice network through updating their computerized dialing devices.

15 As a derivative of the described system, an updateable electronic telephone directory system can be also implemented. In this case a customer's phone set would include a computerized dialing device with electronic memory containing a conventional telephone directory and a personal directory as well. This telephone directory can be periodically updated on-line by the telephone company.

20 Easily interceptable systems such as cellular and satellite telephone systems, in addition to the protection described above, can be protected from "cloning" when their signals can be intercepted and the "identity" of the phone can be cloned for gaining unauthorized access and use of the system by unauthorized parties.

25 Mobile telephone and mobile communications systems are protected in a manner similar to networks or land based telephone systems. In this instance, the novel and improved method of changing cyber coordinates is designed to reliably protect mobile phone systems from unauthorized use commonly known as cloning as well as to make intercept of wireless communications more difficult than it is at present. With this system the static wireless phone number or other similar identifier is not used for identification and authorization. Instead, a set of private identifiers is generated known only to the phone company and base stations
30 controlling mobile phone calls and used to continually update the mobile phone and base station directories with current valid identifiers. This approach provides vastly superior

protection over current methods requiring that each call be intercepted in order to track and keep current with changing identifiers. Immediate detection of unauthorized attempts to use a cloned phone is realized and law enforcement may be notified in near real time for appropriate action.

5 Other electronic devices using wireless communications can be protected by the methods and systems described above.

Finally, computers often contain databases with a variety of information. That information in a database often has wide-ranging levels of sensitivity or commercial value. This creates a situation when large computers serve multiple users with vastly different levels
10 of access. Furthermore, even within the same level of access, security considerations require compartmentalization of information when each user has to have access to only a small portion of the database.

The existing systems try to solve this situation by utilizing passwords and internal firewalls. As it was mentioned earlier, password-based systems and firewalls are not
15 sufficient against computerized attacks. In practical terms it means that a legitimate user with a low level of access, utilizing hacking techniques from his station, potentially can break into even the most restricted areas of the database.

This problem can be solved by using the method of the present invention. A piece of information such as a file or a directory in a computer exists in cyber space. Accordingly, it
20 has its cyber address, usually expressed as a directory and/or a file name which defines its position in a particular computer file system. This, in effect, represents the cyber coordinates of that piece of information within a computer.

As described earlier, information security can be provided if a system manager periodically changes the directories and/or file names in the system, i.e. the cyber addresses
25 of the information, and notifies only appropriate parties of the current file names. This method would ensure that each user computer knows locations of only files to which it has legitimate access. Furthermore, a user would not even know of existence of the files to which he has no access.

To further strengthen the system and make it user-friendly, the user would have a
30 personal directory similar to an address book, where only permanent directory and/or file names are accessible to him, while the variable side of the "address book" would be

accessible only to the system manager and upgraded periodically. In this arrangement variable directory and/or file names can contain any required level of entropy, further increasing resistance to attacks from within the system. Additionally, an internal “router” or “filter” can also perform information security monitoring functions, detect intrusion attempts and issue appropriate alarms in real time.

Obviously, in order to ensure information security in such arrangement any computer-wide search by keywords or subject should be disabled and substituted with a search within specific clients’ “address books”.

The systems and methods described above allow for creation of a feasible infrastructure protection system such as a national or international infrastructure protection system. When detected at specific points cyber attacks are referred to such a system for further analysis and a possible action by law enforcement authorities.

I claim:

1. A method for protecting a communications device which is connected to a communications system against an unauthorized intrusion which includes:

5 providing the communications device with at least one identifier,
providing the at least one identifier for use in accessing the communications device to entities authorized to access said communications device,

sensing the presence or absence of said identifier before granting access to said communications device,

10 providing access to said communications device when the use of said at least one correct identifier is sensed

denying access to said communications device and providing said communications device with at least one new identifier when the absence of the correct at least one identifier is sensed during an attempt to access said communications device, and providing said at least
15 one new identifier to entities authorized to access said communications device.

2. The method of claim 1 which includes periodically changing the at least one identifier and providing the changed at least one identifier to the entities authorized to access said communications device.

20 3. The method of claim 1 which includes providing said communications device with a plurality of separate identifiers,

sensing the presence or absence of all of said plurality of identifiers before granting access to said communications device,

25 providing access to said communications device when the use of all of said identifiers is sensed, and

denying access to said communications device and providing said communications device with a new plurality of identifiers to replace the previous plurality of identifiers when the absence of any one of the correct identifiers is sensed.

30 4. The method of claim 3 which includes periodically changing said plurality of

separate identifiers and providing the changed identifiers to the entities authorized to access said communications device.

5 5. The method of claim 1 which includes permitting a predetermined number of attempts to access said communications device with a correct at least one identifier after the absence of the correct at least one identifier is sensed before providing said communications device with at least one new identifier,

 and providing access to said communications device if the correct at least one identifier is sensed during the predetermined number of attempts to access.

10

 6. The method of claim 2 wherein said communications system is a telephone system and said communications device is a telephone.

 7. The method of claim 1 wherein said communications system is a computer network with said entities authorized to access said communications device being authorized computers having access to said computer network, said communications device including at least one host computer having access to said computer network.

15

 8. The method of claim 7 which includes periodically changing the at least one identifier for the host computer and providing the changed at least one identifier to the authorized computers.

20

 9. The method of claim 7 which includes providing the authorized computers with an unchangeable, accessible address for the host computer which is used by the authorized computer to activate and transmit the at least one identifier for the host computer when the authorized computer initiates access to the host computer.

25

 10. The method of claim 8 which includes providing each authorized computer with an authorized computer identifier,

30

 providing the host computer with a destination identifier,

 causing each authorized computer to access said host computer with at least a host

computer destination identifier and the authorized computer identifier,

sensing the presence or absence of both said host computer destination identifier and an authorized computer identifier before granting access to said host computer,

5 providing access to said host computer when the use of both a correct host computer destination identifier and an authorized computer identifier is sensed, and

denying access to said host computer and providing said host computer with a new host computer destination identifier when the absence of either a correct host computer destination identifier or a correct authorized computer identifier is sensed.

10 11. The method of claim 10 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination identifier and an authorized computer identifier after the absence of a correct host computer destination identifier or an authorized computer identifier is sensed before providing said host computer with a new host computer destination identifier, and

15 providing access to said host computer if correct host computer destination and authorized computer identifier are sensed during the predetermined number of attempts to access the host computer.

20 12. The method of claim 11 which includes storing said host computer destination identifier as an inaccessible identifier in said authorized computers, and providing said authorized computers with an unchangeable, accessible host computer address, which will activate and transmit the host computer destination identifier when an authorized computer initiates access to the host computer.

25 13. The method of claim 8 which includes providing said host computer with a host computer destination identifier and a host computer port identifier,

causing each authorized computer to access said host computer with at least the host computer destination identifier and the host computer port identifier,

30 sensing the presence or absence of both said host computer destination identifier and said host computer port identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer

destination identifier and a correct host computer port identifier are sensed, and

denying access to said host computer and providing said host computer with a new destination identifier and port identifier when the absence of either or both of a correct host computer destination or port identifier is sensed.

5

14. The method of claim 13 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination and port identifier when either or both an incorrect host computer destination or port identifier is sensed before providing said host computer with a new destination and port identifier, and

10

providing access to said host computer if both correct host computer destination and port identifiers are sensed during the predetermined number of attempts to access said host computer.

15

15. The method of claim 14 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computers and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

20

16. An intrusion protection method for protecting a host computer connected to a computer communications system which includes one or more authorized computers having access to said computer communications system which are authorized to access said host computer which includes:

25

providing each authorized computer with an authorized computer identifying address,
providing said host computer with a host computer destination identifier and a host computer port identifier,

providing said host computer destination identifier and said host computer port identifier to said authorized computers,

30

causing each authorized computer to access said host computer with the host computer destination and port identifiers and said authorized computer identifying address,
sensing the presence or absence of said host computer destination and port identifiers

and said authorized computer identifying address before granting access to said host computer,

providing access to said host computer when the use of correct computer destination and port identifiers and a correct authorized computer identifying address is sensed, and

5 denying immediate access to said host computer when the absence of any one or more of the correct host computer destination and port identifiers or the authorized computer identifying address is sensed.

17. The method of claim 16 which includes periodically changing the host computer destination and port identifiers and providing these changes to the authorized computers.

18. The method of claim 17 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

19. The method of claim 16 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

20. The method of claim 16 which includes permitting a predetermined number of attempts to access said host computer with correct host computer destination and port identifiers and a correct authorized computer identifying address after the absence of at least a correct one of said identifiers and authorized computer identifying address is sensed by the host computer and

providing access to said host computer if correct host computer destination and port identifiers and a correct authorized computer identifying address are sensed during the predetermined number of attempts to access said host computer.

21. The method of claim 19 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

22. The method of claim 20 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

23. The method of claim 22 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

24. A method of communication with a remote entity over a communication system which includes

providing the remote entity with at least one remote entity cyber coordinate identifier, providing the remote entity cyber coordinate identifier to one or more base entities authorized to communicate with said remote entity,

periodically changing the remote entity cyber coordinate identifier to a new remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

25. The method of claim 24 which includes changing the remote entity cyber coordinate identifier to a new cyber coordinate identifier in response to an attempt to communicate with said remote entity with an incorrect remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

FIG. 1

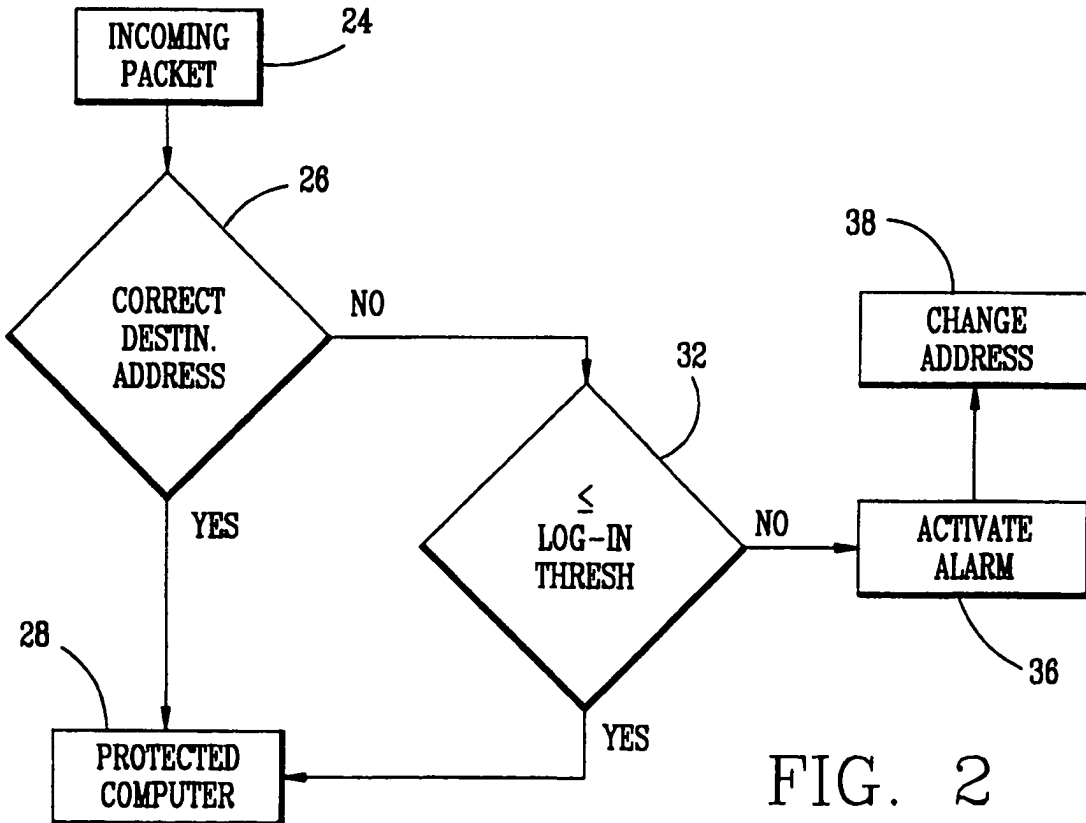
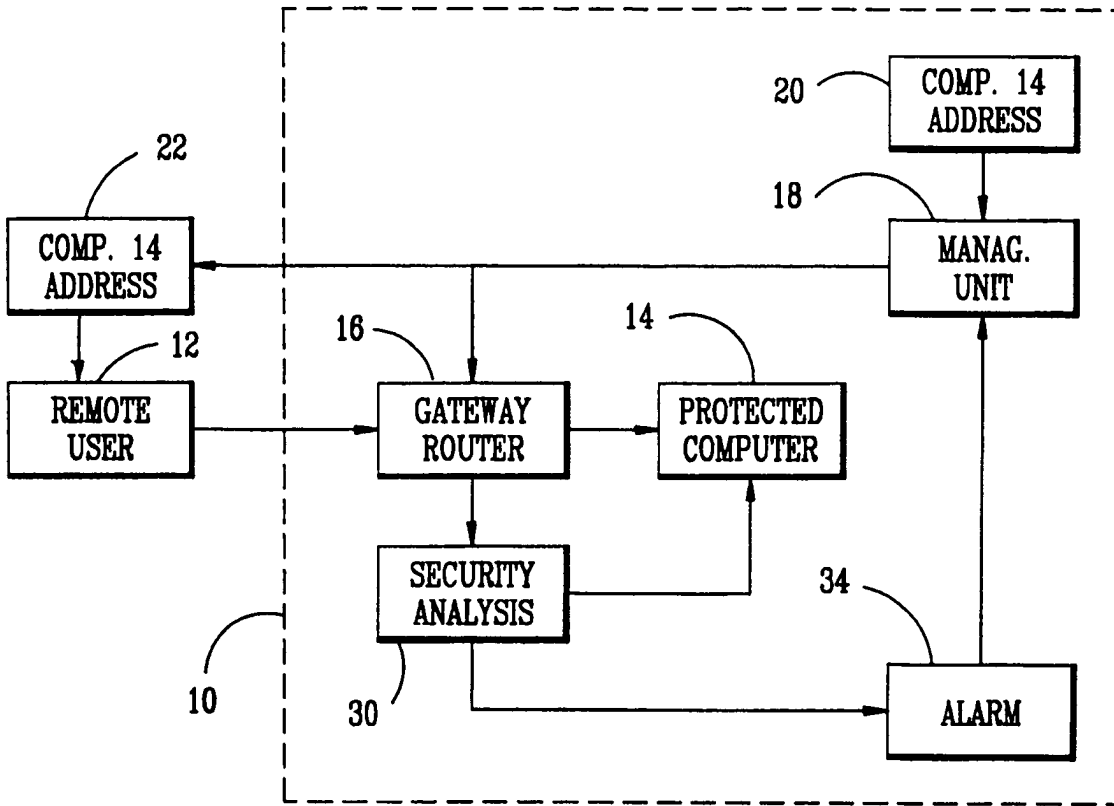


FIG. 2

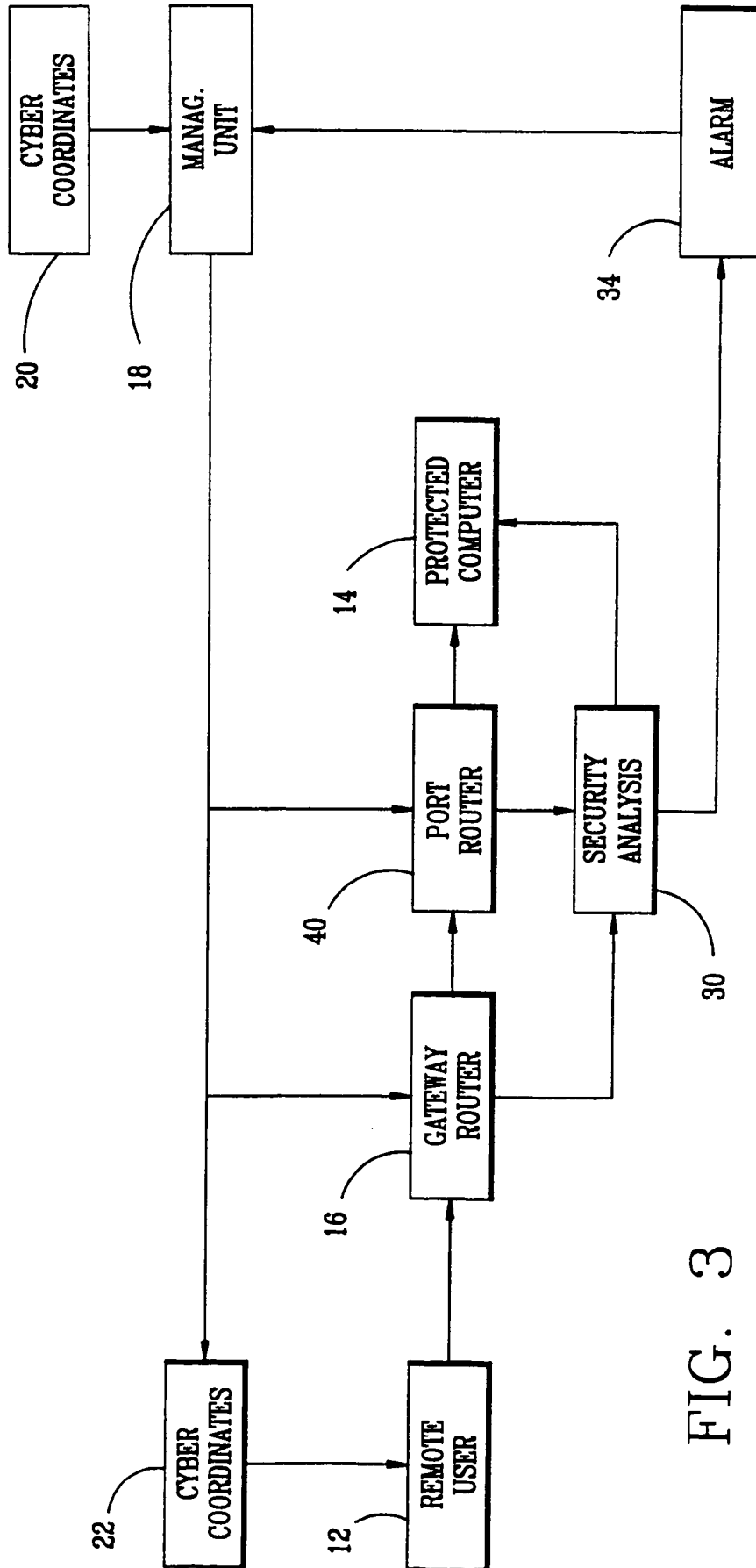
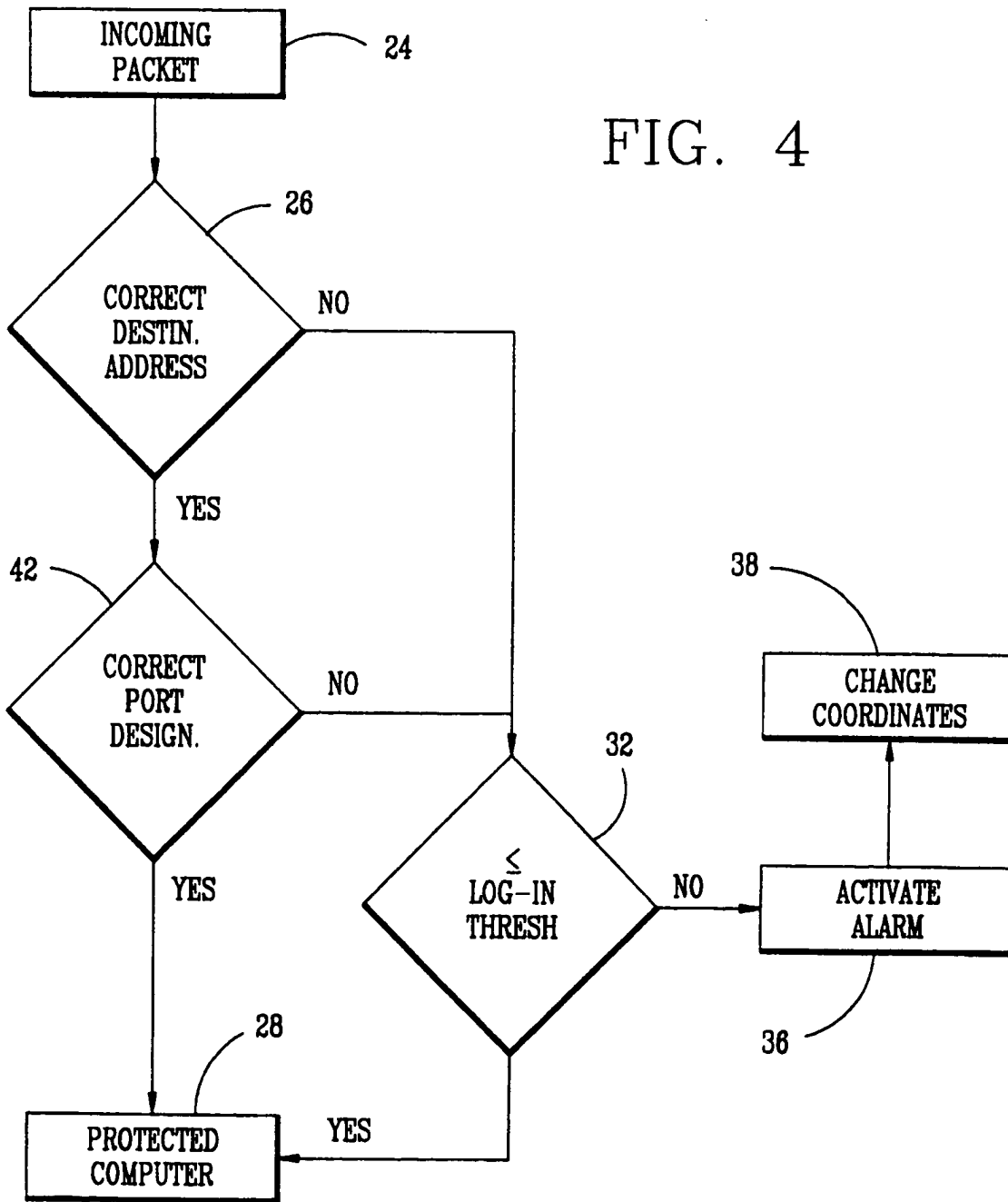


FIG. 3

FIG. 4



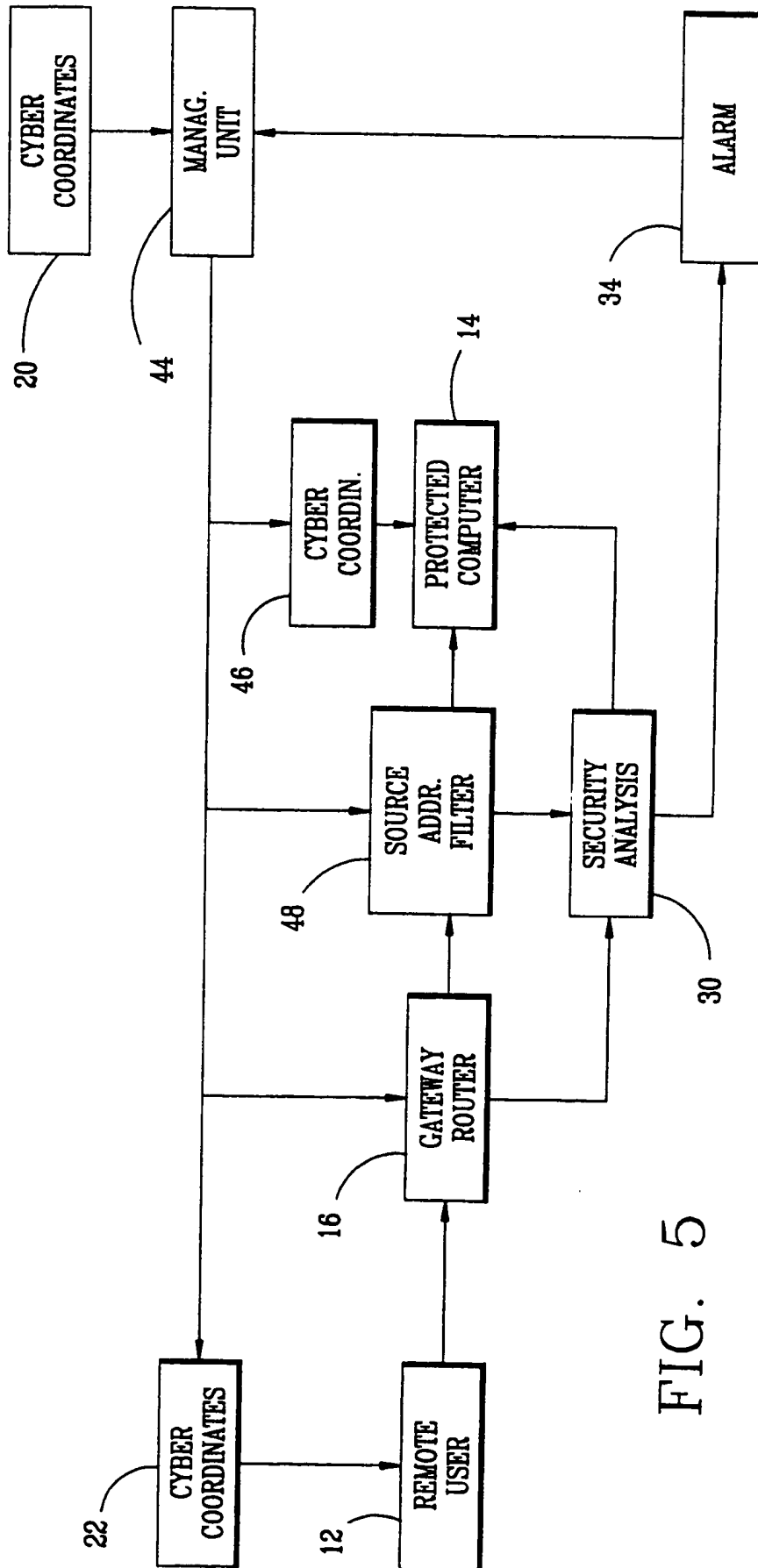


FIG. 5

FIG. 6

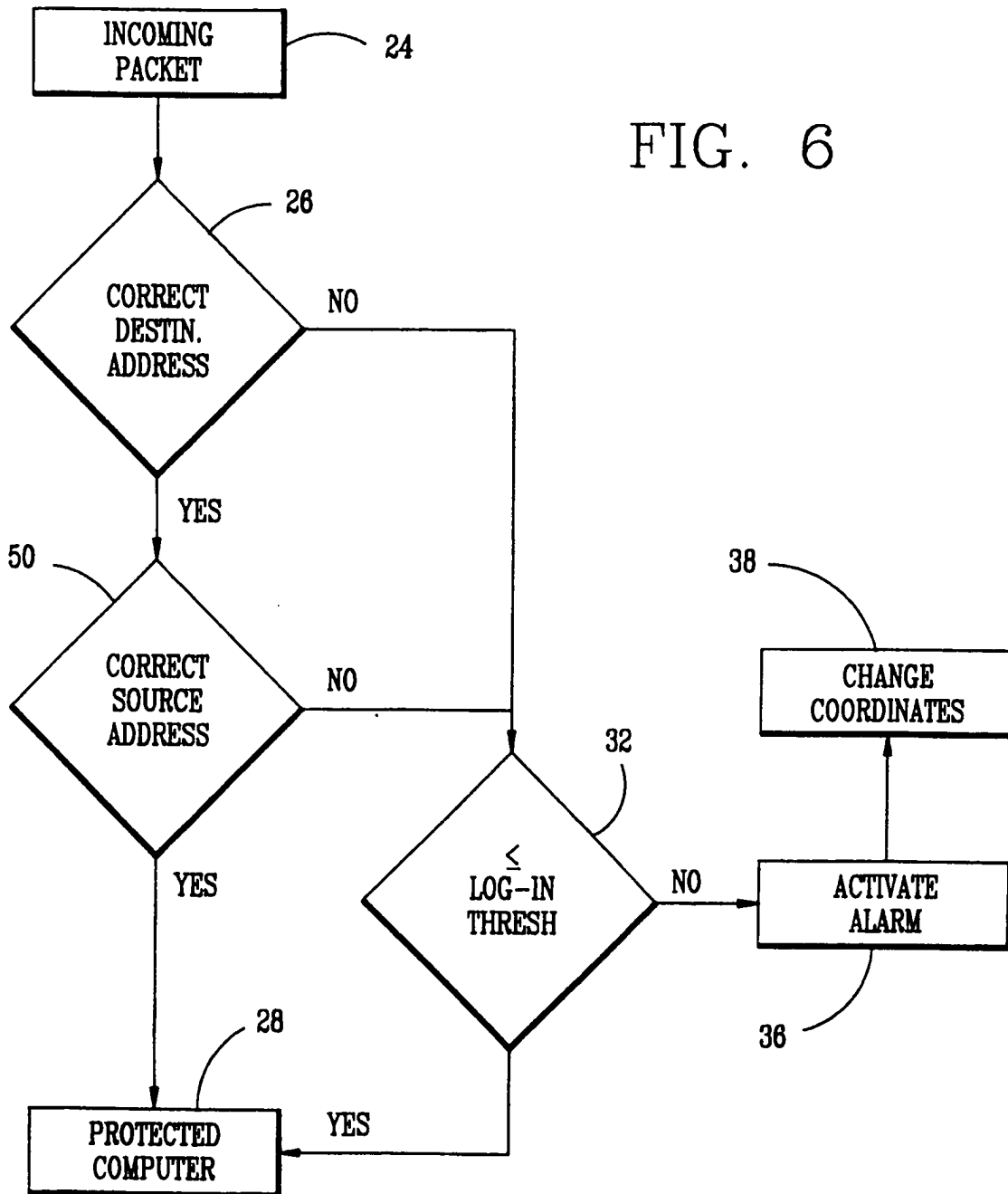
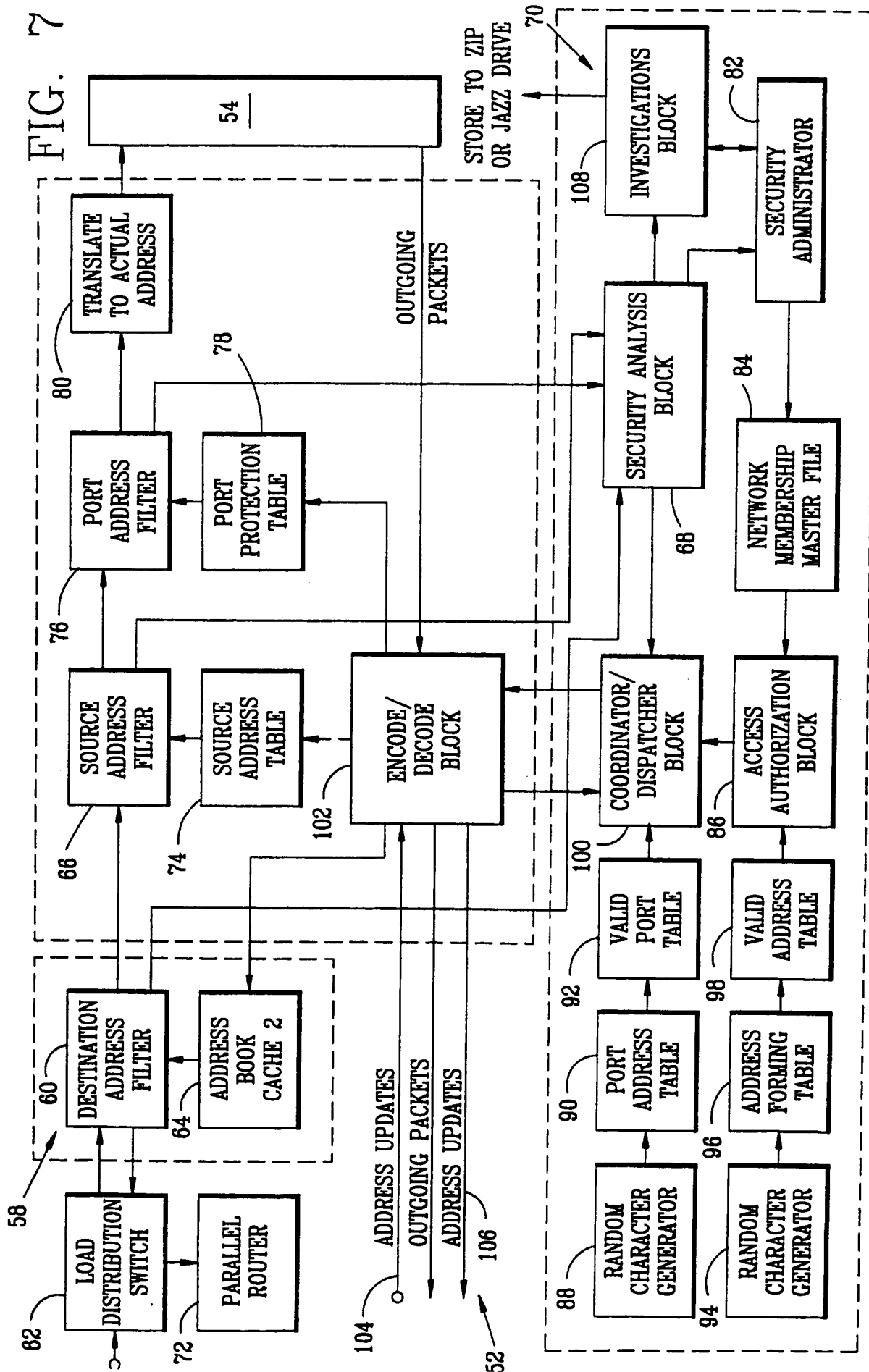


FIG. 7



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/00
US CL : 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/201,200,202; 340/825.31,825.34; 380/255;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS US PATENT FILE; WEST; JPAB; EPAB; DWPI; TDBD;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,805,801 A (HOLLOWAY ET AL) 08 SEPTEMBER 1998, Entire document.	1-25
Y	US 5,796,942 A (ESBENSEN) 18 AUGUST 1998, Entire document.	1-25
Y,P	US 5,905,859 A (HOLLOWAY ET AL) 18 MAY 1999, Entire document.	1-25
Y	US 5,892,903 A (KLAUS) 06 APRIL 1999, Entire document.	1-25
A	US 5,537,099 A (LIANG) 16 JULY 1996, Entire document.	1-25
A	US 5,278,901 A (SHIEH ET AL) 11 JANUARY 1994, Entire document.	1-25

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
E earlier document published on or after the international filing date	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*a* document member of the same patent family
O document referring to an oral disclosure, use, exhibition or other means	
P document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

20 JULY 2000

Date of mailing of the international search report

22 AUG 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

NADEEM IQBAL

Telephone No. (703) 308-5228

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,881 A (CONKLIN ET AL) 23 NOVEMBER 1999, Entire document.	1-25

CORRECTED VERSION

B1002

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
8 March 2001 (08.03.2001)

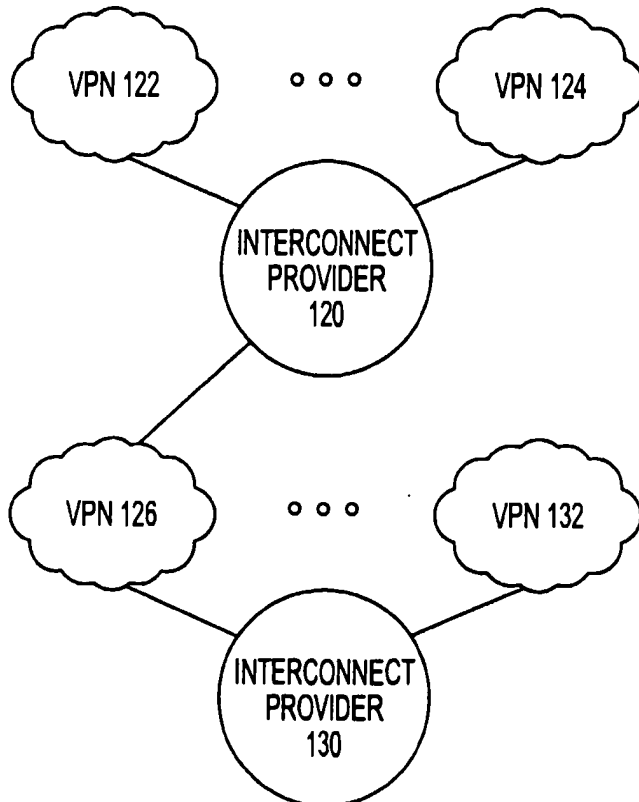
PCT

(10) International Publication Number
WO 01/016766 A1

- (51) International Patent Classification⁷: G06F 13/00
- (21) International Application Number: PCT/US00/23774
- (22) International Filing Date: 31 August 2000 (31.08.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/151,563 31 August 1999 (31.08.1999) US
- (71) Applicant: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).
- (72) Inventors: WHITTLE, Bryan; 73 Zion-Wertsville Road, Skillman, NJ 08558 (US). TESINK, Kaj; 140 Park Road, Fair Haven, NJ 07704 (US).
- (74) Agents: ROBINSON, Douglas, W. et al.; Banner & Witcoff, Ltd., Eleventh Floor, 1001 G Street, N.W., Washington, D.C 20001-4597 (US).
- (81) Designated States (*national*): AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS



(57) Abstract: A system and method for interconnecting multiple VPNs (122, 124, 126, 132), each using multiple service providers (120, 130), while offering a minimum standard of end-to-end connection quality and reliability. The system and method utilizes an overseer that resolves end-to-end issues across multiple interconnected virtual private networks (122, 124, 126, 132). When connecting multiple virtual private networks (122, 124, 126, 132) multiple interconnect providers (120, 130) are interconnected so that the end-to-end service quality standard. The certification of service providers, exchange points, transit service providers and IPsec devices permits interoperability for encryption, integrity and authentication across the product of all IPsec vendors. When two subscribers both use certified IPsec equipment then they can provide each other with controlled access to each other's networks.



WO 01/016766 A1



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(48) Date of publication of this corrected version:

12 September 2002

(15) Information about Correction:

see PCT Gazette No. 37/2002 of 12 September 2002, Section II

**SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL
PRIVATE NETWORKS**

5 This application claims priority to the following provisional patent applications, which are incorporated herein by reference in their entireties:

 (1) Provisional Application Serial No. 60/151,563, titled "Method & Apparatus For a Globalized Automotive Network & Exchange," filed on August 31, 1999, and having reference no. 99,532 (479.83581).

10

BACKGROUND OF THE INVENTION

Field of the Invention

 The present invention relates to virtual private networks. More particularly, the present invention relates to virtual private networks wherein in each virtual private network, multiple service providers can be utilized by the trading partners of the
15 virtual private network. The end-to-end service quality of the connection within the virtual private network is guaranteed to meet minimum requirements. The end-to-end service quality encompasses numerous factors including: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. The system and method of the present
20 invention is directed to the interconnection of multiple virtual private networks each having multiple service providers. Furthermore the present invention encompasses a system and method for interconnecting multiple interconnect providers, such as exchange points, exchange networks, direct connect or transit service providers, between the multiple virtual private networks. Finally, the present invention employs
25 an end-to-end overseer across the multiple virtual private networks.

Description of the Related Art

 Early in 1994, the automotive industry recognized the need for global network services that would support more new demanding automotive business applications. The purpose of this network service was to simplify complex, redundant, outdated
30 connection methods while minimizing costs and ensuring the management, security, reliability, and performance essential to the automotive industry. Transport Control Protocol/Internet Protocol (TCP/IP) was endorsed as the standard suite for electronic data communications.

Ultimately in 1995, the industry formed a Telecommunications Project Team to oversee the design and development of a common global communication infrastructure supporting automotive industry application initiatives (later called the Automotive Network eXchange (ANX) Implementation Task Force). The Task Force, in June 1997, published the initial results of the technical design process for this new network service, called the Automotive Network eXchange (ANX), in "ANX Release 1 Draft Document Publication" (TEL-2 01.00). This reference is incorporated herein by reference in its entirety. The TEL-2 specification undergoes constant updating and correction.

The ANX system is a business-to-business communications infrastructure that provides a uniform, secured link between trading partners, such as manufacturers and suppliers, in the automotive industry. The ANX is a subscription-based network composed of Certified Service Providers (CSP). CSPs are providers of IP network service that have satisfied certain service end-to-end quality. CASPs are certificate authority service providers. The Certified Exchange Point Operator (CEPO) provides services to interconnect CSPs. CEPOs also must satisfy certain end-to-end service quality requirements.

Trading Partners (TP) are registered end users, or subscribers, of the ANX system such as automotive parts manufacturers, suppliers, original equipment manufacturers, and car manufacturers. The ANX system allows TPs to communicate, exchange information, and transact business with other TPs over the ANX network. The TP may utilize any TCP/IP-compliant application program to exchange information with other TPs. The registered TP selects the TPs with which it wants to communicate and thereafter may gain access to and receive communications from those selected TPs. As a result, the ANX system allows each TP to develop its own virtual private network with its customers and vendors.

The ANX system significantly reduces the complexity of connecting to multiple trading partners. Since there are diverse communication protocols for the trading partners, separate links are required to access each trading partner.

By having a single private network operated under a uniform protocol, interconnectivity between various trading partners is substantially simplified. In addition, ANX offers improved end-to-end service quality. For example, if an auto manufacturer needs to place with its parts supplier an order for car seats, the

manufacturer may submit over the ANX system its confidential CAD drawings directly to the supplier. The manufacturer may also fill out the order form that the supplier may have for filling orders and timely submit over the ANX system due to its high reliability and performance.

5 The CSP and the CEPO must satisfy certain performance and security requirements in order to be certified under the ANX. The certification process is disclosed in ANX Release 1 Document Publication (TEL-2 02.00), which is incorporated herein by reference in its entirety.

The ANX VPN permits the use of a plurality of different IPsec devices. By
10 virtue of the TEL-2 specification and the certification process all of the designated IPsec device are guaranteed to communicate with one another across the ANX VPN.

While the ANX was originated out of the need to interconnect automotive related companies, it is not limited to that industry. Any company/industry may become a TP, e.g. an aerospace company, a healthcare company, etc. ANX has
15 become known as the Advanced Network eXchange.

With the advent of the Internet, global communication has become a reality. While the Internet works well for non-mission critical applications, such as transmitting and receiving e-mail and hosting websites, it has some drawbacks for business-to-business commerce and communication that require stringent end-to-end
20 service quality. Quality concerns are in the area of end-to-end service quality as explained previously.

For example, when two companies want to communicate over the Internet, the lag between the systems at each company will be different virtually every time. The connection each has through their service provider, i.e. 14.4K, 28.8K, 56K, ISDN,
25 DSL, T1, etc., plus the number of servers through which the connection is directed contribute to the resulting time lag between the two companies. Depending upon the type of information transmitted, the two parties may require a maximum acceptable time lag. Due to the nature of the Internet, it cannot guarantee such a maximum time lag. Furthermore, the two companies may desire that service assistance be available
30 at certain times or 24 hours a day. The Internet has no such guarantees for help availability in a multi-provider environment. Such a lack of guaranteed bandwidth, latency and reliability are major impediments to business-to-business commerce and communication over the Internet.

In recent years the number of electronic viruses and hacker attacks has increased dramatically. A company considering conducting business-to-business commerce over the Internet runs the risk of making their intranet vulnerable to such viruses and attacks with the potential related loss of data.

5 In order to address the security issue, some companies have developed virtual private networks (VPNs). Secure VPNs permit a company to communicate with any other entity on the network without the risk of increased vulnerability to viruses and hackers. However, while VPNs can connect to other VPNs over the Internet by providing authentication, access control, confidentiality and data integrity, there is
10 still no way the end-to-end quality of the connection can be guaranteed to meet a required set of minimum standards in a multi-provider setting.

A secure VPN is a communication network that is secured with encryption and authentication. Secure VPNs are based on multiple technologies, for example IPsec, tunneling, certification and shared secret authentication. IPsec is the security
15 standard established by the Internet Engineering task Force (IETF). Tunneling permits private networks to cross the Internet using unregistered IP addresses.

SUMMARY OF THE INVENTION

From the foregoing, it is desirable to provide a system and method for interconnecting multiple VPNs each using multiple service providers while offering a
20 minimum standard of end-to-end service quality.

The system and method of the present invention utilizes an overseer that defines the service quality, continually qualifies service providers as meeting that service quality, and resolves end-to-end issues across multiple interconnected virtual private networks, such as the ANX. When connecting multiple virtual private
25 networks according to the system and method of the present invention multiple interconnect providers are interconnected, and the manner in which these interconnect providers are interconnected so that the quality and reliability standards is met are another aspect of the present invention.

Certification of IPsec devices permits interoperability for encryption, integrity
30 and authentication across the product of all IPsec vendors. When two subscriber companies both use certified IPsec equipment then they can provide each other with controlled access to each other's networks.

Based on the foregoing, an object of the present invention is to provide a system and method of interconnecting multiple VPNs each using multiple service providers while offering a minimum standard of end-to-end connection quality and reliability.

5 Another object of the present invention is to provide a system and method of interconnecting multiple VPNs having an overseer that resolves end-to-end issues across multiple virtual private networks.

Still another object of the present invention is to provide a system and method of connecting multiple virtual private networks in which multiple interconnect
10 providers are interconnected so that the end-to-end service quality is met.

DETAILED DESCRIPTION OF THE DRAWINGS

The foregoing and other attributes of the present invention will be described with respect to the following drawings in which:

15 **Fig. 1** is a block diagram of two interconnected virtual private networks according to the present invention;

Fig. 2 is a configuration of governance and management of separate virtual private networks;

20

Fig. 3 is a configuration of governance and management of interconnected virtual private networks according to the present invention;

Fig. 4 is an interconnection configuration for governance of multiple inter-
25 connected virtual private networks according to the present invention;

Fig. 5 is a flow chart showing contractual obligations according to the present invention;

30 **Fig. 6** is a diagram illustrating end-to-end latency in a virtual private network having multiple service providers;

Fig. 7 is a diagram illustrating end-to-end availability in a virtual private network having multiple service providers;

Fig. 8 is a diagram illustrating trouble handling in a virtual private network
5 having multiple service providers;

Fig. 9 is a diagram illustrating an accountability model for a single virtual private network having multiple service providers;

Fig. 10 is a diagram illustrating an accountability model for multiple virtual
10 private networks having multiple service providers according to the present invention;

Fig. 11 is a diagram illustrating end-to-end interconnection of two virtual private networks according to the present invention;

15

Fig. 12 is a diagram illustrating a trouble escalation model for interconnection of two virtual private networks according to the present invention;

Fig. 13 is a diagram illustrating a multiple virtual private network fee model
20 for interconnection of two virtual private networks according to the present invention;
is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;

Fig. 14 is a diagram illustrating interconnection of two virtual private
25 networks using a single transit certified service provider according to the present invention;

Fig. 15 is a diagram illustrating interconnection of two virtual private
networks using a multiple transit certified service providers according to the present
30 invention;

Figs. 16 is a diagram illustrating interconnection of multiple virtual private networks using a multiple transit certified service providers, where no single transit

certified service provider connects all of the virtual private networks according to the present invention; and

Figs. 17a - c are alternative configurations for interconnecting multiple virtual
5 private networks according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 shows a block diagram of two interconnected virtual private networks 20 and 22. The present system and method of the interconnecting multiple virtual private networks is not intended to be limited to only these types of networks and has applicability to a wide variety of virtual private networks.

Each virtual private network 20 and 22 is shown having a trading partner (TP) 24 and 26, respectively. While Fig. 1 shows only one TP 24 and 26 for each virtual private network, there can in fact be hundred or thousands of such TPs for each virtual private network. Fig. 1 is intended to define the end-to-end service quality concept, and for such a purpose, only one TP 24 and 26 is need for each virtual private network 20 and 22.

The end-to-end service quality, provided by the present system and method of interconnecting multiple virtual private networks, cannot be achieved by simply interconnecting two virtual private networks, such as 20 and 22, with a wire. The end-to-end service quality incorporates a user-centric philosophy, where the user is the TP or subscriber. The user is guaranteed a minimum level of service encompassing factors that include: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. Simply connecting the two virtual private networks 20 and 22 with a wire will not achieve the minimum satisfactory levels for these factors.

To achieve such minimum levels of satisfactory performance for these factors the system and method must include a way to resolve disputes between the two virtual private networks. Referring to Fig. 2, each VPN 20 and 22 is shown as having its own governance, program management, coepetition policy, contracts, service assurance, and service description. While each virtual private network can operate with a successful level of end-to-end service quality when each VPN is not interconnected to another VPN, the governance, program management, coepetition policy, contracts, service assurance, and service description may need to be revised when interconnecting two or more VPNs in order to maintain the end-to-end service quality. It will be appreciated that at the very least the interconnection of at least two VPNs adds at least one additional level of complexity with regard to service between the VPNs.

One resolution is shown in Fig. 3, in which each VPN 20 and 22 maintain their own governance, but the program management, cooperation policy, contracts, service assurance, and service description for the two VPNs 20 and 22 are unified. Such unification means that where the parameters for the program management, cooperation policy, contracts, service assurance, and service description of the two VPNs 20 and 22 are different, the parameter used in one of the networks is chosen as the acceptable minimum standard or a compromise parameter different from the parameter used in each or the VPNs is agreed upon. It is possible that the parameters for communication within each VPN need not change, while the new parameters are used only when communicating between VPNs. Fig. 3 further shows that the system and method contemplate connecting more than two VPNs.

One configuration for governance of multiple interconnected VPNs is shown in Fig. 4. In this scenario each VPN has its own program overseer (POVER) 30, and a global, or multiple virtual private network, overseer 32 is provided to resolve issues between the POVERs 30. Arrows are shown between the POVERs 30 indicating that the POVERs 30 are free to resolve their issues without requiring the GOVER 32. The GOVER is called on when direct POVER-to-POVER resolution fails. Each of the POVERs 30 governs one of the regional VPNs, while the GOVER 32 oversees the interconnection of the VPNs.

The GOVER is responsible for end-to-end quality assurance, and in particular acts as an inter-VPN interconnection certifier. The GOVER certifies interconnection facilities, and certifies a global CASP-CASP trust model. The GOVER also is an inter-VPN arbitrator that steps in when POVERs cannot resolve trouble between them.

Since the VPNs are used to running their networks in isolation, the interconnection of multiple VPNs has unique issues such as resolving trouble and conflicts between the VPNs and maintenance of minimum end-to-end service quality across the multiple programs. Since the system and method of the present invention are directed to providing specific end-to-end service quality, it must be possible for TPs to quantify the end-to-end service quality levels, and these service quality levels must be sufficient to allow applications to work across the multiple VPNs. Therefore, a high level of metric compatibility and measurement techniques are required.

In the ANX type VPN each TP, CSP and CEP must meet specified criteria to become certified and to maintain that certification. The certification provides the TPs or subscribers with confidence that the level of transport and security will meet their business needs. The ANX type VPN utilizes multiple CSPs. On one level it is easier to run a VPN where all TPs are required to use a single CSP. The use of multiple CSPs in the ANX type VPN fosters competition between the CSPs and allows the VPN to reach TPs that may not be serviced by a single CSP. The implementation of multiple CSPs, however, brings with it the drawback of insuring that the CSPs can talk to one another. Whether the connection from one TP to another TP within the same VPN is through a single CSP or two CSPs should be invisible to the TPs. The TPs need never know when one or more CSPs are used for any particular connection. The certification process ensures that the TPs use one of the certified IPsec devices at their premises, and that the CSPs will utilize certified equipment and meet certain metrics so as to achieve the end-to-end service quality guaranteed to the TPs. In this manner, the multiple CSPs will be able to communicate with one another. The CSPs must meet business criteria, technical metrics, ongoing monitoring, trouble-handling criteria, routing registry criteria, and domain name registry criteria to achieve and maintain certification.

Fig. 5 shows the contractual obligations of the members of an ANX-type VPN. The TPs contract with the VPN, as denoted in Fig. 5 by the arrows to the overseer, and contract with one of the multiple CSPs. The CSPs contract with the VPN and with the CEPO. The CEPO contracts with the VPN. Each entity is responsible for the services that that entity provides.

The technical metrics for achieving end-to-end service quality in the ANX-type network include among other metrics, latency and availability. Fig. 6 illustrates the end-to-end latency within the ANX network. The TP1 router is connected to ANX CSP₁, which in turn is connected to ANX CEPO. TP2 router is connected to ANX CSP₂, which is connected to ANX CEPO. The packet latency from each router through the corresponding CSP is 125 msec. The latency through the ANX CEPO is on the order of microseconds. The total packet latency through the network is therefore only slightly more than 250 msec.

Fig. 7 illustrates the end-to-end availability metric. The Access network between the TP1 router and the ANX CSP₁ is permitted to be unavailable 43.80

hours/year. The ANX CSP₁ 62 may only be unavailable 2.63 hrs./year. The trunk 65 between the ANX CSP₁ 62 and the ANX CEPO may only be unavailable 1.76 hrs./year. The ANX CEPO may only be unavailable 0.44 hours/year. The foregoing availabilities yield a total of 99.895% availability or 9.22 hours per year downtime.

5 The outline for how trouble is handled within the ANX-type VPN is shown in Fig. 8. There are effectively five layers of trouble handling. At the first level trouble between TPs is handled directly between the two TPs. Similarly, issues between the TPs and the CSPs are handled between the two parties. CSPs and the CEPOs also resolve their troubles between the troubled parties. A network overseer is provided to
10 handle troubles that cannot be handled in the foregoing scenarios. The overseer can take complaints from the TPS, the CSPs, and the CEPOs.

A key to providing predictable end-to-end service quality is that the TPs must know the level of service they receive. To this end four service provider accountability levels exist. First, service providers, both interconnect providers and
15 CSPs, must timely fix infrequent service provider troubles. Second, there must be end-to-end service provider cooperation to handle any troubles. Third, recourse must be provided to resolve disputes in the event of disagreement between CSPs and/or interconnect providers. Fourth, recourse must be provided to resolve continued non-compliance with the end-to-end service quality.

20 Referring to Figs. 9 and 10, charts for single VPN and interconnected VPNs are shown, respectively. In Fig. 9, the CSPs 70, CEPOs 72 and CASPs 74 are accountable to the POVER 76. The POVER 76 is accountable to the body 78 representing the TPs. The body 78 is accountable a regional/national arbitration body 80. Where multiple VPNs are interconnected in Fig. 10, the CSPs 70, the CEPOs 72,
25 and CASPs 74 are accountable to the POVERs 76. The POVERs 76 are accountable to a GOVER 77, which in turn is accountable to the body 78. The body 78, instead of being accountable to the regional/national arbitration body 80, is accountable to an international arbitration body 82.

30 The GOVER/POVER model is but one way to oversee ensuring of the end-to-end service quality and metric compatibility. How the ANX-type networks are connected will be discussed below. In this context there must be five key types of end-to-end technology compatibility: 1 network interconnection that ensures a trading partner on one VPN can reach any trading partner on the other VPN; 2 routing

compatibility that ensures any trading partner on one VPN can logically reach any TP on the other VPN; 3 naming compatibility, e.g. so the web names or e-mail names of any trading partner on one VPN can be resolved to an address that is routable over the two VPNs; 4 IPsec compatibility; and 5 digital security certificate compatibility across multiple VPNs. While Figs. 9 and 10 refer to regional/national VPNs and international arbitration, the VPNs need not be limited to a specific country or geographical area. Any ANX-type VPN, regardless of the location of its subscribers could be interconnected.

While Fig. 1 illustrated the interconnection of two VPNs 20 and 22, a significant element is missing. Fig. 11 shows two VPNs, that have multiple service providers, which are connected through an inter-program service provider, also called an interconnect provider. The Tel-2 specification is still used as the basic guide in determining the end-to-end service quality, however regional or particular VPN peculiarities, referred to as deltas, must be considered when establishing the interconnected end-to-end service quality standards.

Returning to the GOVER/POVER model for overseeing interconnected VPNs; Fig. 12 illustrates an end-to-end trouble escalation model. It is expected that CSPs will work together to resolve trouble before contacting a POVER. Similarly, the POVERs and/or the POVERS and the interconnect provider are expected to work together to resolve trouble before contacting the GOVER.

When expanding from a single VPN to interconnected VPNs the inherent costs of running the system naturally increase. How such costs are distributed is an important part of the system. As shown in Fig. 13, the POVERs pay fees to the GOVER to offset the costs of maintaining the GOVER. The VPNs having multiple service providers in turn pay fees to support the POVER. Furthermore the interconnect providers pay a certification fee to the GOVER for certification as a interconnect provider between VPNs.

There are multiple methods of interconnecting multiple VPNs with interconnect providers. As shown in Fig. 14, all the VPNs, having multiple service providers, can be interconnected using a single interconnect provider. Alternatively, all the VPNs can be interconnected by multiple interconnect providers, as shown in Fig. 15, thereby creating competition between the interconnect providers, just as there is competition between the CSPs in a single xNX-type VPN. Finally, as shown in

Fig. 16, where no suitable interconnect provider is available to connect all the VPNs having multiple service providers, multiple interconnect providers are used. These interconnect providers service different combinations of VPNs. In Fig. 16, interconnect provider 120 interconnects VPNs having multiple service providers 122, 124, and 126. Interconnect provider 130 interconnects VPNs having multiple service providers 132 and 126. As a result, a TP of VPN 132 must connect through both Interconnect provider 130 and Interconnect provider 120 to reach TPs of either VPN 122 or 124.

How the multiple VPNs interconnect will directly affect the resulting end-to-end service quality. Figs. 17a-c illustrate potential configurations of multiple VPNs. In Fig. 17a a first TP 200 connects to a first CSP 210. The CSP210 connects to a first exchange point 220. The TP 200, CSP 210, and the exchange point 220 are within a first VPN 240. A second TP 250 connects to a second CSP 260, which connects to a second exchange point 270. The TP 250, CSP 260 and exchange point 270 are within a second VPN 280. The two VPNs 240 and 280 are interconnected by an Interconnect provider 300, which is connected to the exchange points 220 and 270.

In Fig. 17b TP 200, CSP 210, exchange point 220 and Interconnect provider 300 are connected in the same manner shown in Fig. 17a. While the second TP 250 is connected to the CSP 260, the exchange point 270 is not provided. Instead CSP 260 is shown as connecting directly to the Interconnect provider 300. This embodiment encompasses the situation where the Interconnect provider 300 and CSP 260 are the same entity or are directly wired. Fig. 17c is similar to Fig. 16b, Except that the interconnect provider also acts as a CSP 320, and a third TP 310 is connected directly to the Interconnect provider 300/CSP 320.

As stated previously, while the end-to-end service quality is based upon the TEL-2 specification, the degree to which the TEL-2 specification needs to be modified to interconnect multiple VPNs depends upon the chosen complexity of the interconnection. An xNX-type VPN uses a maximum of two CSPs between any two TPs. A larger value, either three or four, is needed for multiple VPNs. The Interconnect provider will account for one additional CSP, and for configuration set forth in Fig. 16, two Interconnect providers are employed in addition to the two CSPs yielding four CSPs.

Having described several embodiments of the system and method for interconnecting multiple virtual private networks in accordance with the present invention, it is believed that other modifications, variations and changes will be suggested to those skilled in the art in view of the description set forth above. It is
5 therefore to be understood that all such variations, modifications and changes are believed to fall within the scope of the present invention as defined in the appended claims.

What is claimed is:

1. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:
5 at least one interconnect provider for connecting said multiple virtual private networks,
 said multiple virtual private networks connected through said at least one interconnect provider having minimum standards for cross network services, virtual private network interoperability, inter-network performance, inter-network reliability,
10 disaster recovery and business continuity, inter-network security, inter-network customer care, and inter-network trouble handling.
2. A system as recited in claim 1, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.
15
3. A system as recited in claim 1, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.
- 20 4. A system as recited in claim 1, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.
- 25 5. A system as recited in claim 1, wherein each of said multiple virtual private networks comprises a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks.
- 30 6. A system as recited in claim 5, further comprising a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks.
7. A system as recited in claim 6, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

8. A system as recited in claim 5, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

5

9. A system as recited in claim 6, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

10. A system as recited in claim 1, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

15

11. A system as recited in claim 1, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

20. A method of interconnecting multiple interconnection providers between multiple virtual private networks, each of said virtual private networks having multiple subscribers, multiple service providers and at least one exchange point interconnecting said multiple service providers, with guaranteed end-to-end service quality, comprising the steps of:

25. providing at least one interconnect provider disposed between a first set of said multiple service providers in one of said multiple virtual private networks and a second set of multiple service providers in a second one of said multiple virtual private networks.

30. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein one of said at least one transit service providers is also one of said multiple service providers within at least one of said multiple virtual private networks.

14. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, further comprising the step of certifying all of said multiple service providers in all of said multiple virtual private networks, said multiple transit service providers, and said exchange points to ensure minimum end-to-end quality and security levels are maintained.

15. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, comprising the further step of providing at least one exchange point between a first set of said multiple service providers in one of said multiple virtual private networks and said at least one interconnect service provider.

16. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein a maximum number of service providers between two subscribers within one of said multiple virtual private networks is two, and the maximum number of said service providers and transit service providers between subscribers of different ones of said multiple virtual private networks is three.

17. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 15, further comprising the step of providing at least one second exchange point between a second set of said multiple service providers in another one of said multiple virtual private networks and said at least one transit service provider.

18. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:
at least one interconnect provider for connecting said multiple virtual private networks,
each of said multiple virtual private networks comprising a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks, and

a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks,

5 said multiple virtual private networks connected through said at least one interconnect provider have: minimum standards for cross network services; virtual private network interoperability; inter-network performance; inter-network reliability; disaster recovery and business continuity; inter-network security; inter-network customer care; and inter-network trouble handling.

10 19. A system as recited in claim 18, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.

15 20. A system as recited in claim 18, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.

21. A system as recited in claim 18, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.

20 22. A system as recited in claim 18, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

25 23. A system as recited in claim 18, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

30 24. A system as recited in claim 18, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

25. A system as recited in claim 18, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect

providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

- 5 26. A system as recited in claim 18, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

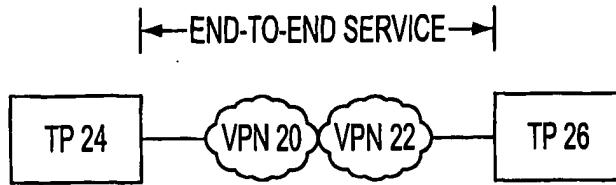


FIG. 1

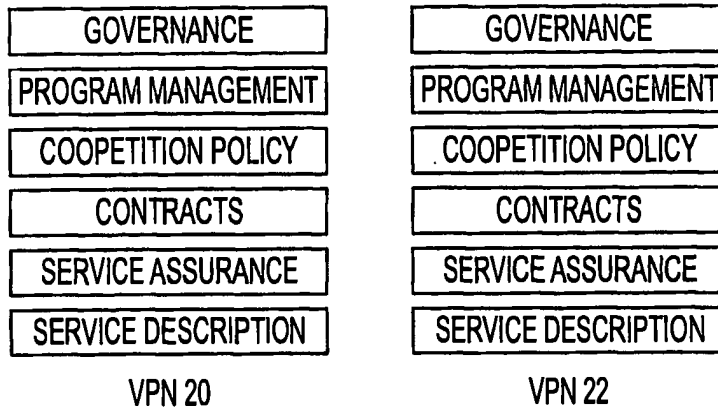


FIG. 2

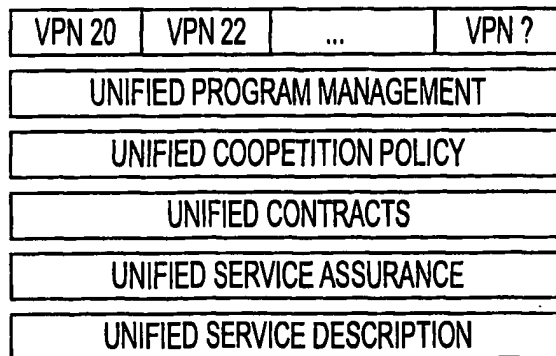


FIG. 3

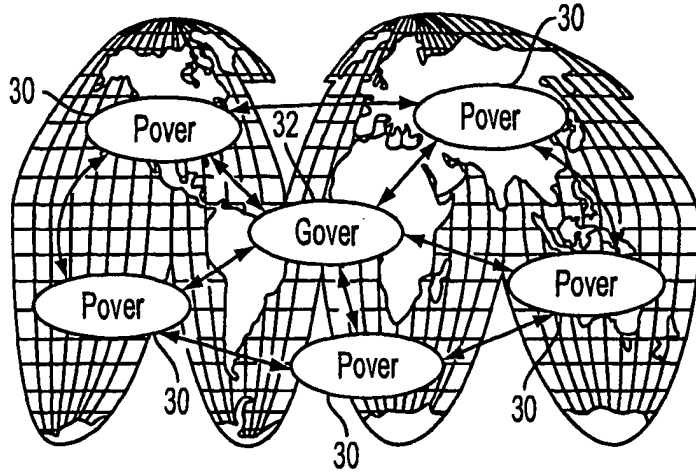


FIG. 4

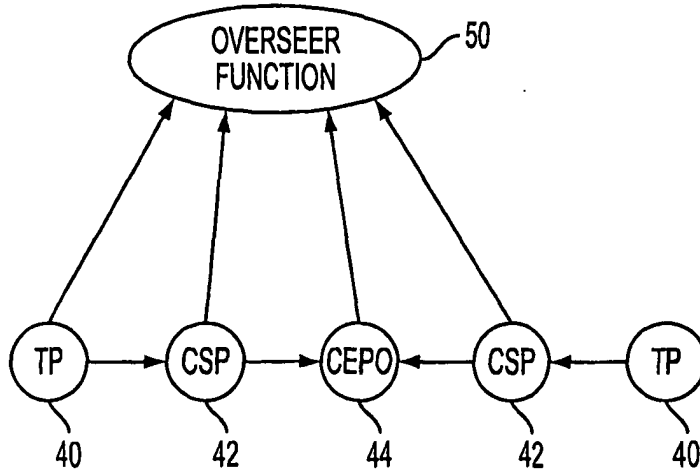


FIG. 5

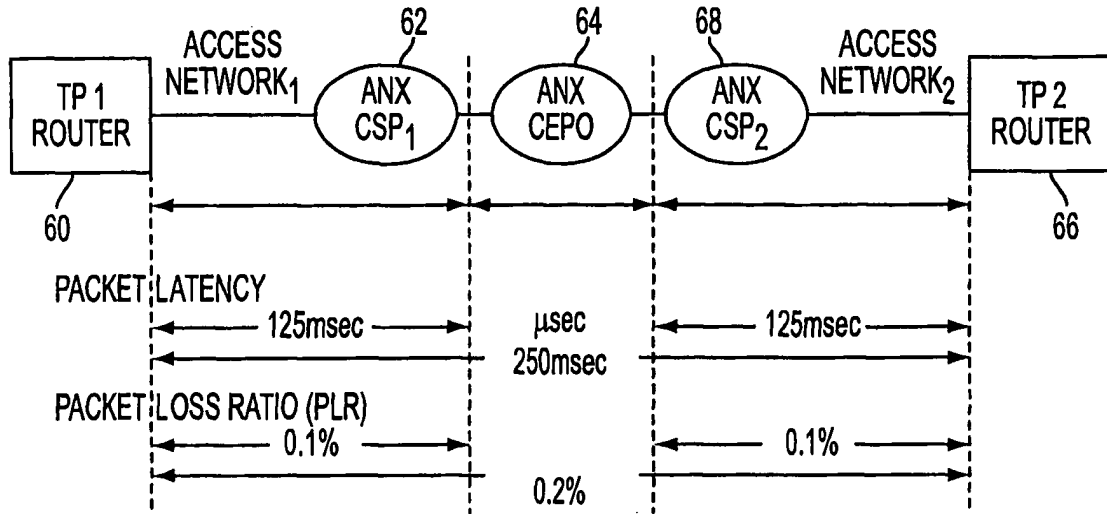


FIG. 6

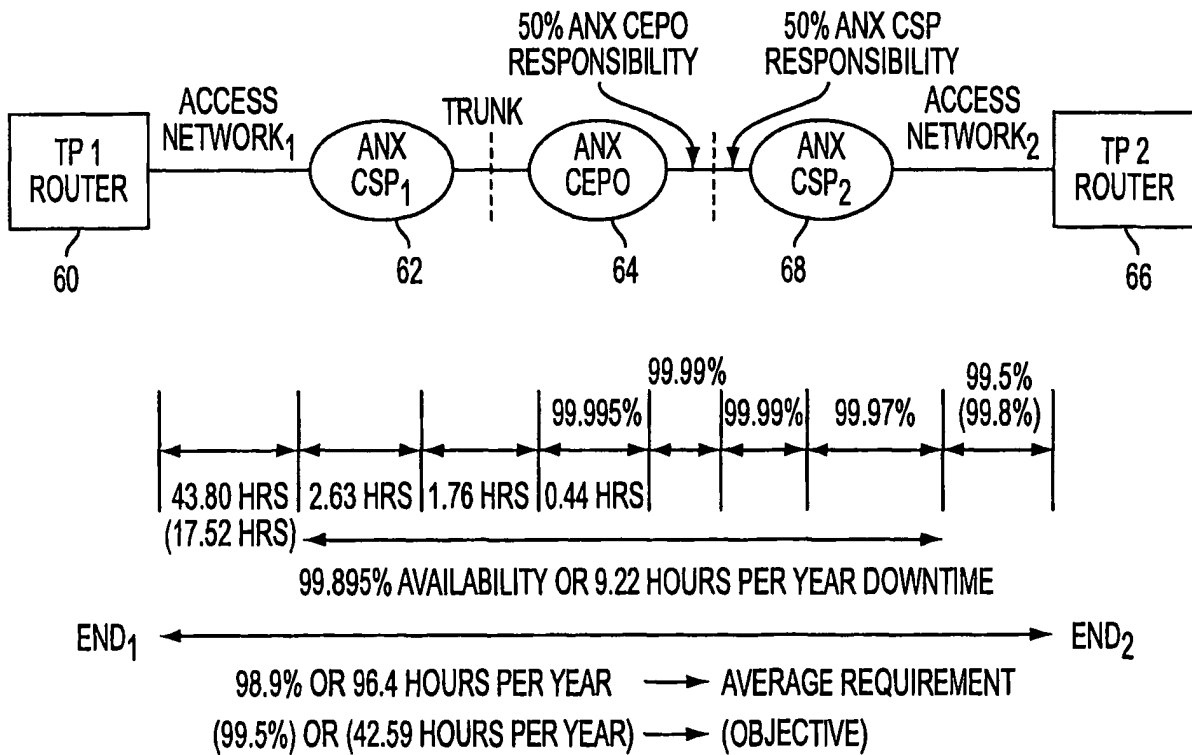


FIG. 7

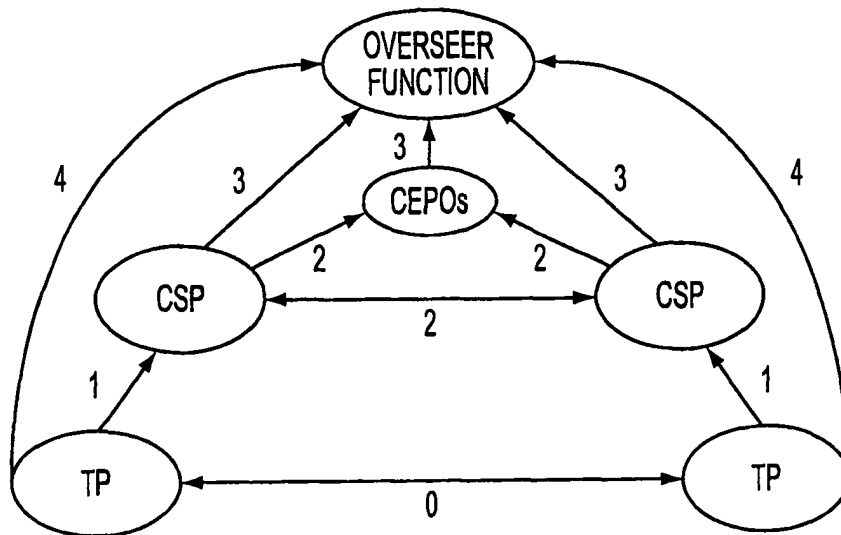


FIG. 8

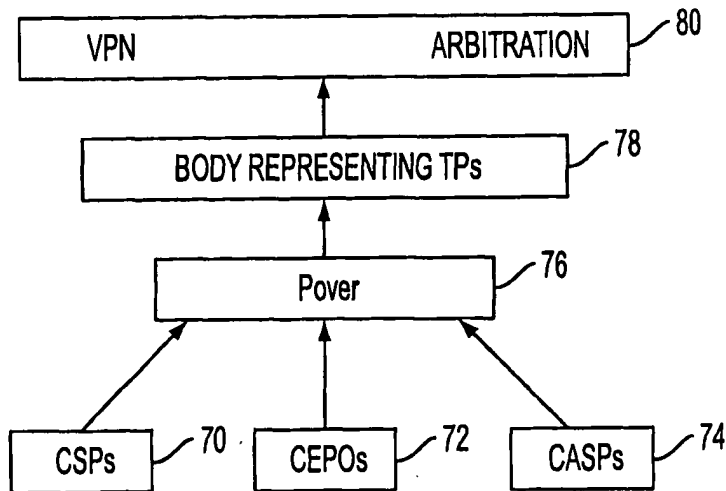


FIG. 9

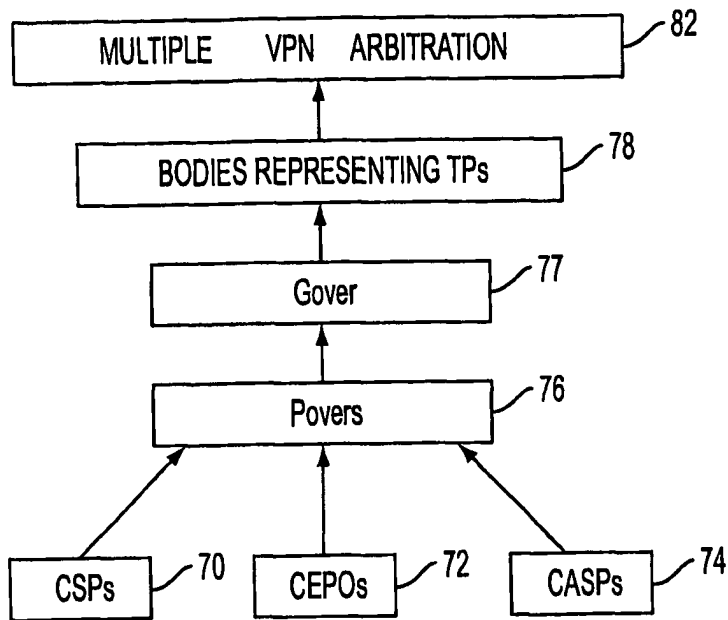


FIG. 10

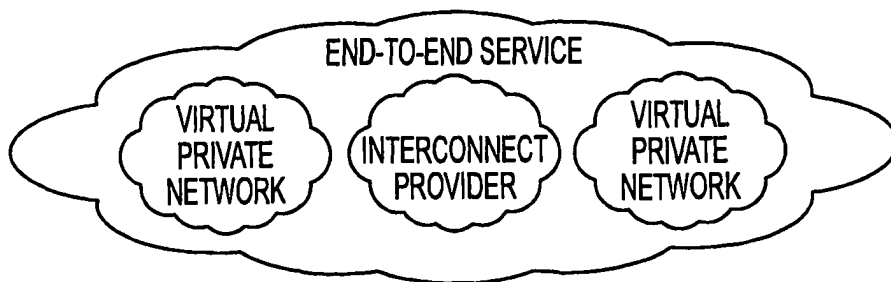


FIG. 11

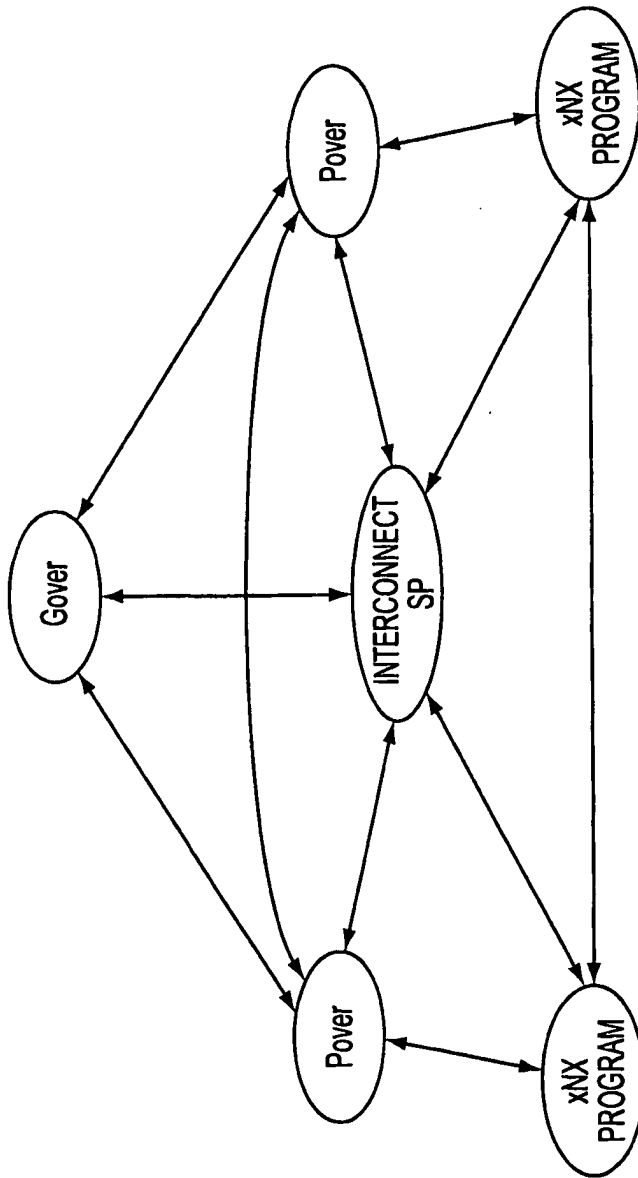


FIG. 12

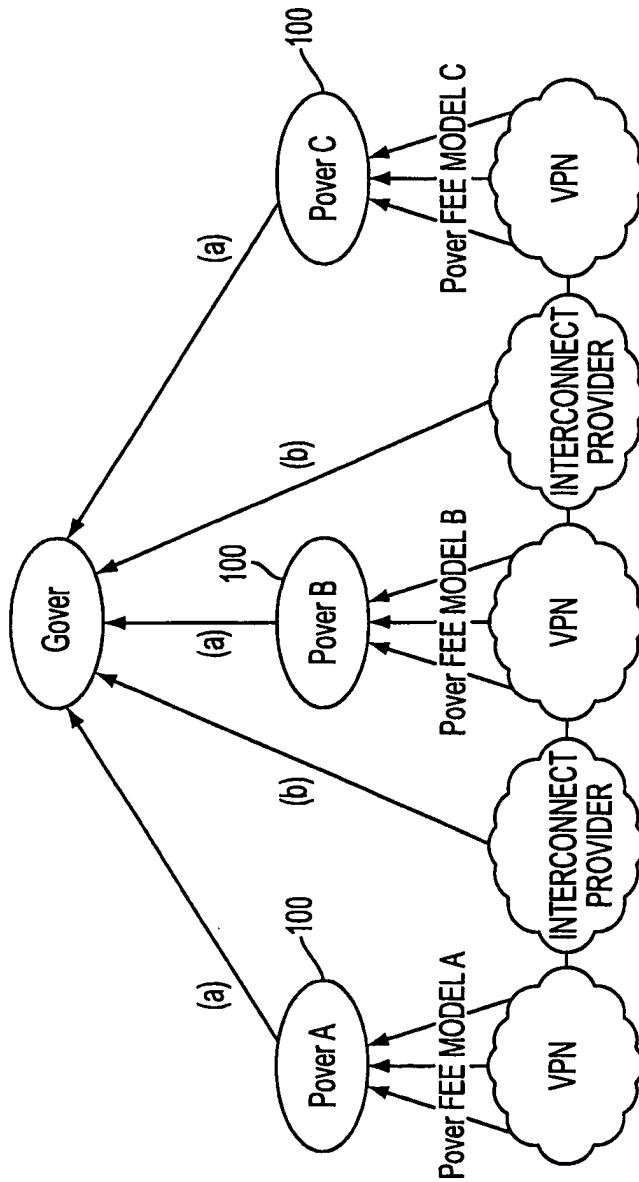


FIG. 13

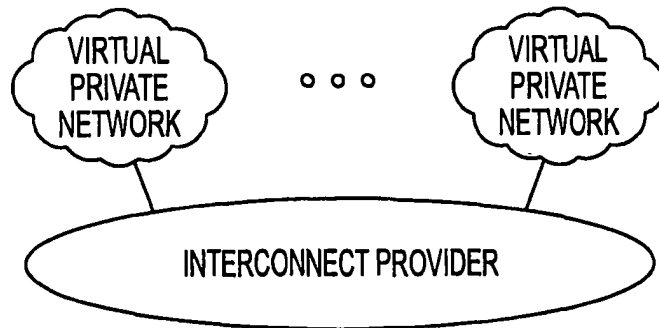


FIG. 14

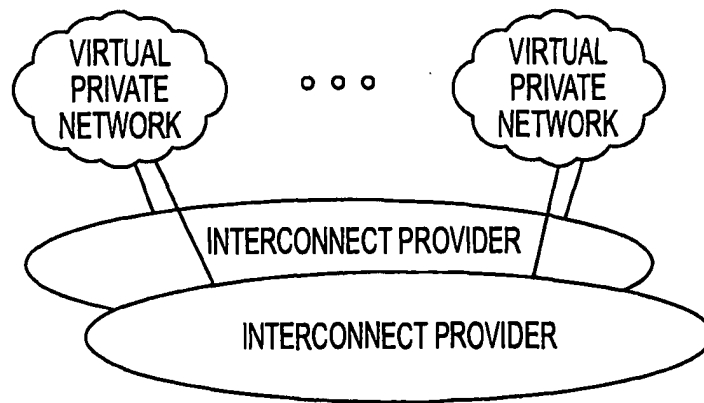


FIG. 15

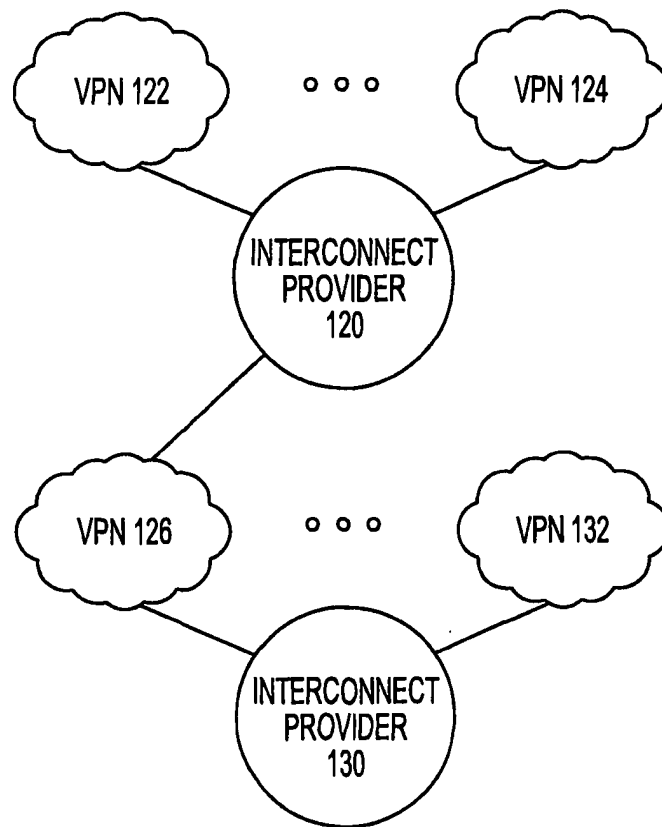


FIG. 16

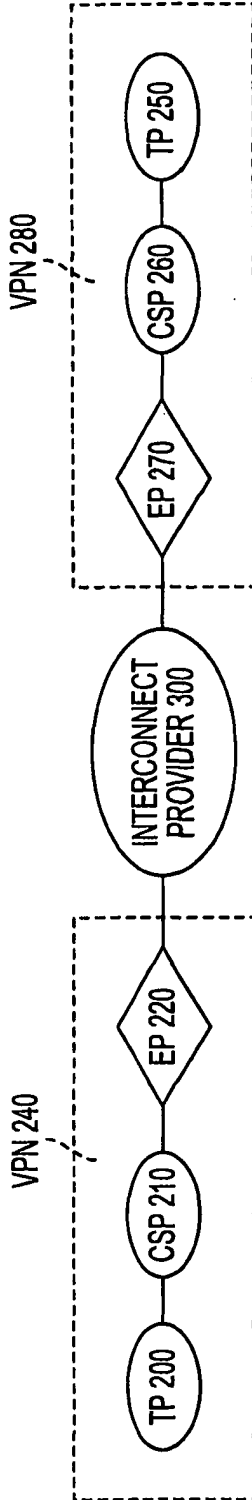


FIG. 17A

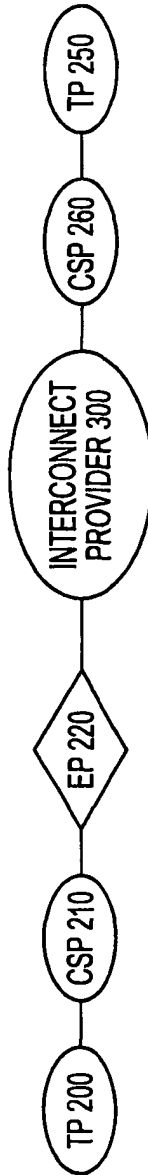


FIG. 17B

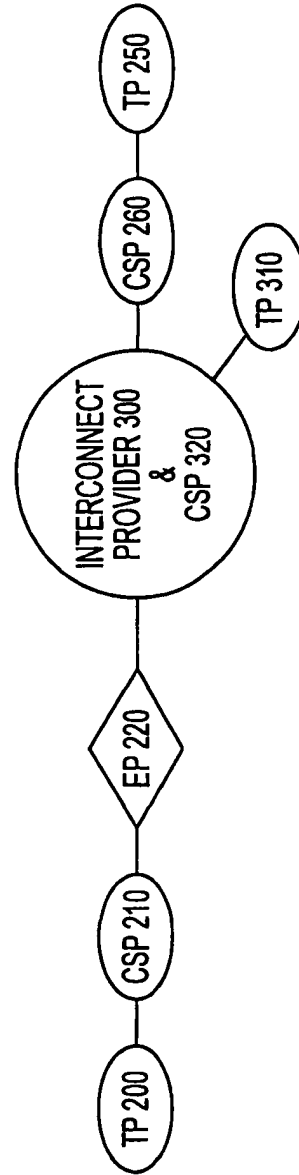


FIG. 17C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/23774

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00

US CL : 709/201, 220, 221, 223, 227, 228, 236, 238

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/201, 220, 221, 223, 227, 228, 236, 238

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CAS ONLINE
service(1w)providers, private(1w)(networks or lans), interconnection(1w)provider

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 6,104,701 A (AVARGUES et al) 15 August 2000, Figs 1-3, col 1, lines 60-67, col 2, lines 1-6, lines 22-67, col 3, lines 1-6, col 6, lines 20-67, col 7, lines 1-26.	1-26

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
E earlier document published on or after the international filing date	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*G* 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

10 OCTOBER 2000

Date of mailing of the international search report

26 OCT 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

MOUSTAF A M. MEKY

Telephone No. (703) 305-9697

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

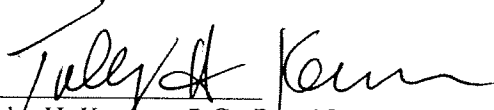
In the Reexamination of:)	
Victor Larson, et al.)	
)	
U.S. Patent No.: 7,188,180)	
Filed: November 7, 2003)	Examiner:
Issued: March 6, 2007)	Andrew L. Nalven
)	
For: METHOD FOR ESTABLISHING)	Group Art Unit: 3992
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF VIRTUAL)	
PRIVATE NETWORK)	
)	
Reexamination Proceeding)	
Control No.: 95/001,270)	
Filed: December 8, 2009)	

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Information Disclosure Statement, the Information Disclosure Citation, and references cited in the Information Disclosure Citation, which were filed with United States Patent and Trademark Office on February 23, 2010, were served this 25th day of February, 2010 on Requester by causing a true copy of same, in electronic format saved on a DVD, to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP



Toby H. Kusner, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Atabak R. Royae, Reg. No. 59,037
McDermott Will & Emery LLP
Attorneys for Patent Owner

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

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
Date: February 25, 2010

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re-Exam
Application
Control No. 95/001,270

Confirmation No. 2128

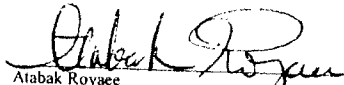
Based on U.S.
Patent No. 7,188,180
First Named Inventor Victor Larson

Issued: 06/06/2007

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

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 2/23/10.


Atabak Royace

Examiner: Andrew L. Nalven

Art Unit 3992

Mail Stop: Inter Partes Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

- 1) Information Disclosure Statement (2 pages)
- 2) Information Disclosure Statement by Applicant (Form 1449) (19 pages);
- 3) Copies of references listed in the IDS Form 1449 as follows:

References	Express Mail Tracking No
Box 1 containing references B1000-B1002 & C998-C1060;	EV643770648US
Box 2 containing references C1061-C1080;	EV643770951US
Box 3 containing references C1081-C1105;	EV643770665US
Box 4 containing references C1106-C1152;	EV643770679US
Box 5 containing references C1153-C1205;	EV643770682US
Box 6 containing references C1206-C1212; and	EV643770696US
Box 7 containing references C1213-C1242	EV643770705US

- 4) Return receipt postcard.

Attorney Docket No. 077580-0090
Re-exam Application Control No. 95/001,0270
Re: U.S. Patent No. 7,188,180

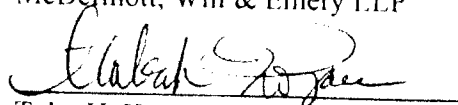
PATENT

There are no fees due with the filing of this Information Disclosure Statement. However, the Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Date: February 23, 2010

Respectfully submitted,

McDermott, Will & Emery LLP



Toby H. Kusmer, Reg. No. 26,418

Atabak R. Royae, Reg. No. 59,037

McDermott Will & Emery LLP

28 State Street

Boston, MA 02109-1775

Telephone: (617) 535-4065

Facsimile: (617) 535-3800

BS199 1643958-1 077580 0090

Docket No.: 077580-0090

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re-Exam
Application
Control No.

95/001,270

Confirmation No. 2128

Based on U.S.

Patent No. 7,188,180
First Named Inventor Victor Larson

Issued: 06/06/2007

Inventor

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

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 2/23/07.

Examiner: Andrew L. Nalven

Art Unit 3992


Arabak Royace

Mail Stop: Inter Partes Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97, 1.98 and 1.555, 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 reexamination of the above-referenced patent, and that the documents be made of record therein and appear among the "References Cited" on any Re-examined patent to issue therefrom.

Documents A1000-A1039, B1000-B1002 and C998-C1241 listed in the enclosed form PTO-1449 have been produced by Microsoft Corp. in VirnetX Inc. and Science Applications International Corp. v. Microsoft Corp. civil action currently pending before the U.S. District Court for the Eastern District of Texas.

Document C1242 is an Inter Partes Reexamination Request filed for U.S. Patent No. 6,502,135, which is related to the above-referenced patent and is concurrently undergoing reexamination proceedings.

Although the undersigned attorney has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. Enclosed are 7 boxes containing foreign patent documents B1000-B1002 and non-patent literature documents C998-C1242 as indicated in form 1449 enclosed herewith. The Examiner is invited to call the undersigned attorney for any questions regarding any of these documents.

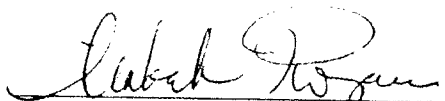
This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands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

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

The commissioner is hereby authorized to charge any fees required 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



Toby H. Kusmer, Reg. No. 26,418
Atabak R. Royace, Reg. No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800
Date: 2/23/2010

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

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

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 1 of 19

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	5,303,302	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	

*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	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 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)			
	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, FreeS/WAN)			
	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, FreeS/WAN)			
	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.	
	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/socswp.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	

*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, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	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)	
	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	
	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 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)	
	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	

*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.			
	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		

*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	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.	
	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-ietf-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," <i>FirstVPN</i> , (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 <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	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.			
	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	Publicly available emails relating to FreeSWAN (MSFTVX00018833-MSFTVX00019206). (FreeSWAN emails, FreeS/WAN)			
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)			
	C1101	Network Associates Gauntlet Firewall For Unix User's Guide Version 5.0 (1999). (Gauntlet User's Guide - Unix, Firewall Products)			
	C1102	Network Associates Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0 (1999) (Gauntlet Getting Started Guide - NT, Firewall Products)			
	C1103	Network Associates Gauntlet Firewall For Unix Getting Started Guide Version 5.0 (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)			
	C1104	Network Associates Release Notes Gauntlet Firewall for Unix 5.0 (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)			
	C1105	Network Associates Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0 (1999) (Gauntlet NT Administrator's Guide, Firewall Products)			
	C1106	Trusted Information Systems, Inc. Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1 (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)			
	C1107	Network Associates Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0 (1999) (Gauntlet NT GVPN, GVPN)			
	C1108	Network Associates Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0 (1999) (Gauntlet Unix GVPN, GVPN)			
	C1109	Dan Sterne Dynamic Virtual Private Networks (May 23, 2000) (Sterne DVPN, DVPN)			
	C1110	Darrell Kindred Dynamic Virtual Private Networks (DVPN) (December 21, 1999) (Kindred DVPN, DVPN)			
EXAMINER			DATE CONSIDERED		

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

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

Subst for form 1449/PTO

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

Complete if Known

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.
	C1111	Dan Sterne <i>et al.</i> TIS Dynamic Security Perimeter Research Project Demonstration (March 9, 1998) (Dynamic Security Perimeter, DVPN)
	C1112	Darrell Kindred Dynamic Virtual Private Networks Capability Description (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 Security Quickstart Task Update (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 DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan (March 10, 1998) (IFD 1.1, DVPN)
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide - Connection Manager, available at 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, available at http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) available at http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), available at http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), available at http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)
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	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.			
	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.mspx (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.mspx (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.mspx (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		

*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.			
	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.mspix (MS PPTP)			
	C1139	Kenneth Gregg, et al., Microsoft Windows NT Server Administrator's Bible 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.mspix (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.mspix (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, NT Network Plumbing: Routers, Proxies, and Web Services 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.mspix (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.mspix (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, F-Secure Evaluation Kit (May 1999) (FSECURE 00000003) (Evaluation Kit 3)			
	C1147	F-Secure, F-Secure NameSurfer (May 1999) (from FSECURE 00000003) (NameSurfer 3)			
	C1148	F-Secure, F-Secure VPN Administrator's Guide (May 1999) (from FSECURE 00000003) (F-Secure VPN 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				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.			
	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)			
	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		

*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.			
	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 Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame</i> (Macmillan Technical 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 Release 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		

*EXAMINER Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

Subst for form 1449/PTO

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

Complete if Known

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.
	C1186	DARPA, <i>Dynamic Virtual Private Network (VPN) Powerpoint</i>
	C1187	GTE Internetworking, <i>Contractor's Program Progress Report (March 16-April 30, 1998)</i>
	C1188	Darrell Kindred, <i>Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization (January 30, 2001)</i>
	C1189	<i>Virtual Private Networking Countermeasure Characterization (March 30, 2000)</i>
	C1190	<i>Virtual Private Network Demonstration (March 21, 1998)</i>
	C1191	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks (VPNs) and Integrated Security Management (2000)</i>
	C1192	Information Assurance/NAI Labs, <i>Create/Add DVPN Enclave (2000)</i>
	C1193	NAI Labs, <i>IFE 3.1 Integration Demo (2000)</i>
	C1194	Information Assurance, <i>Science Fair Agenda (2000)</i>
	C1195	Darrell Kindred et al., <i>Proposed Threads for IFE 3.1 (January 13, 2000)</i>
	C1196	<i>IFE 3.1 Technology Dependencies (2000)</i>
	C1197	<i>IFE 3.1 Topology (February 9, 2000)</i>
	C1198	Information Assurance, <i>Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development (January 10-11, 2000)</i>
	C1199	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation (2000)</i>
	C1200	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.2 (2000)</i>
	C1201	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3 (2000)</i>
	C1202	T. Braun et al., <i>Virtual Private Network Architecture, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)</i>
	C1203	Network Associates Products – <i>PGP Total Network Security Suite, Dynamic Virtual Private Networks (1999)</i>
	C1204	Microsoft Corporation, <i>Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)</i>
	C1205	David Johnson et. al., <i>A Guide To Microsoft Proxy Server 2.0 (1999) (Johnson, Microsoft Prior Art VPN Technology)</i>
	C1206	Microsoft Corporation, <i>Setting Server Parameters (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)</i>

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	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.			
	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)			
	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/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		

*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	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 Invalidation 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

Electronic Acknowledgement Receipt

EFS ID:	7090478
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Atabak R Royaee/Jacqueline Andreu
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	077580-0090
Receipt Date:	25-FEB-2010
Filing Date:	08-DEC-2009
Time Stamp:	16:51:27
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Certificate of Service	Certificate_of_Service_IDS_718 8180.pdf	1773033 <small>8b8d30b4091057a44dae394257040541237cf18</small>	no	24

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.



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	02/25/2010	EXAMINER	
MCDERMOTT WILL & EMERY LLP 28 STATE STREET BOSTON, MA 02109-1775			ART UNIT	PAPER NUMBER

DATE MAILED: 02/25/2010

Please find below and/or attached an Office communication concerning this application or proceeding.



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:

RECEIVED
FEB 25 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)



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

Toby H Kusmer :
MCDERMOTT WILL & EMERY LLP : (For Patent Owner)
28 STATE STREET :
BOSTON MA 02109-1775 :

MAILED
FEB 25 2010
CENTRAL REEXAMINATION UNIT

ROTHWELL, FIGG, ERNST & : (For Third Party Requester)
MANBECK, PC :
1425 K Street NW :
Suite 800 :
Washington, DC 20005 :

In re: Larson et alia : DECISION
Inter Partes Reexamination Proceeding : GRANTING-IN-PART
Control No. 95/001,270 : PETITION FOR EXTENSION
Deposited on: 08 December 2009 : OF TIME
For: US Patent No. 7,188,180 : [37 CFR §§ 1.956 & 1.181]

This is a decision on the 22 February 2010, "Petition for Extension of Time Under 37 CFR § 1.956 to Reply to Office Action in Reexamination" requesting the response period be extended by two (2) months for response to the non-final Office action mailed 19 January 2010. The petition was timely filed with certificate of service.

The petition is before the Director of the Central Reexamination Unit for consideration.

The petition is granted-in-part for the reasons set forth below.

DISCUSSION

The Patent Owner's representative requests the period for response be extended by two (2) months for the non-final Office action mailed 19 January 2010, which set two (2) month's time for filing a response thereto. The petition for extension of time was timely filed on 22 February 2010, together with the \$200.00 petition fee as required by 37 CFR § 1.956 and 37 CFR § 1.17 (g). A certificate of service was provided with the petition.

The request is granted-in-part.

37 CFR § 1.956. Patent owner extensions of time in inter partes reexamination.

The time for taking any action by a patent owner in an inter partes reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified. Any request for such extension must be filed on or before the day on which action by the patent owner is due, but in no case will the mere filing of a request effect any extension. Any request for such extension must be accompanied by the petition set forth in § 1.17(g). See § 1.304(a) for extensions of time for filing a notice of appeal to the U.S. Court of Appeals for the Federal Circuit.

Addressing the requirement of 37 CFR § 1.956 to make a showing of "sufficient cause" to grant an extension request, MPEP § 2665 states, in pertinent part:

As noted above, a request for extension of time under 37 CFR § 1.956 will be granted only for sufficient cause, ...

Evaluation of whether "sufficient cause" has been shown for an extension must be made by **balancing** the desire to provide the patent owner with a fair opportunity to respond, **against** the requirement of the statute, 35 U.S.C. § 314(c), that the proceedings be conducted with special dispatch. ...

Any request for an extension of time in a reexamination proceeding must fully state the reasons therefor. The reasons must include (A) a statement of what action the patent owner has taken to provide a response, to date as of the date the request for extension is submitted, and (B) why, in spite of the action taken thus far, the requested additional time is needed. The statement of (A) must provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.

Prosecution will be conducted by initially setting a time period of at least 30 days or one month (whichever is longer), see MPEP § 2662. First requests for extensions of these time periods will be granted for sufficient cause, and for a reasonable time specified-usually 1 month. The reasons stated in the request will be evaluated, and the request will be favorably considered where there is a factual accounting of reasonably diligent behavior

by all those responsible for preparing a response or comments within the statutory time period. Second or subsequent requests for extensions of time, or requests for more than one month, will be granted only in extraordinary situations. (emphasis added)

Any petition request must include the required petition fee as set forth according to 37 CFR § 1.17 (g) and 37 CFR § 1.956.

MPEP § 2665 Extension of Time for Patent Owner Response (in-part)

Requests for an extension of time in an inter partes reexamination proceeding will be considered only after the first Office action on the merits in the reexamination is mailed. Any request for an extension of time filed prior to the first action will be denied.

The certificate of mailing and the certificate of transmission procedures (37 CFR § 1.8), and the “Express Mail” mailing procedure (37 CFR § 1.10), may be used to file a request for extension of time, as well as any other paper in an existing *inter partes* reexamination proceeding (see MPEP § 2666).

As noted above, a request for extension of time under 37 CFR § 1.956 will be granted only for sufficient cause, and the request must be filed on or before the day on which action by the patent owner is due. In no case, will the mere filing of a request for extension of time automatically effect any extension, because the showing of cause may be insufficient or incomplete. In the prosecution of an *ex parte* reexamination, an automatic 1-month extension of time to take further action is granted upon filing a first timely response to a final Office action (see MPEP § 2272). The automatic extension given in *ex parte* reexamination does not apply to the first response to an Action Closing Prosecution (ACP) in an inter partes reexamination. The reason is that in *inter partes* reexamination, parties do not file an appeal in response to an ACP, and a further Office action (Right of Appeal Notice) will issue even if the parties make no response at all. Thus, there is no time period to appeal running against the parties after the ACP is issued, unlike *ex parte* reexamination where an appeal is due after final rejection and the time is thus automatically extended one month to provide time for the patent owner to review the Office’s response to the amendment before deciding whether to appeal.

Evaluation of whether “sufficient cause” has been shown for an extension must be made by balancing the desire to provide the patent owner with a fair opportunity to respond, against the requirement of the statute, 35 U.S.C. § 314(c), that the proceedings be conducted with special dispatch.

DECISION

The patent owner's representative petitions to extend the period for response by adding two (2) months to the response period under 37 CFR § 1.956. The decision to extend the period for response is evaluated based upon a showing of "sufficient cause." There is always the consideration to balance the need for the patent owner to have a fair opportunity to respond to the Office action between the need for special dispatch.

The non-final Office action was mailed 19 January 2010. The patent owner submitted a timely filed the petition on 22 February 2010 with the appropriate fee and certificate of service.

The petition dated 22 February 2010 articulates the delay in receipt of the Office action (one week), the need for a technical expert as yet unavailable, and various concurrent litigation and proceedings. On balance, the petitioner has demonstrated "sufficient cause" for the purpose of granting one (1) month extension of time.

The petitioner is reminded that requests for more than one (1) month, will be granted only in extraordinary situations.

The petition request to extend the response time is hereby granted-in-part.

A one (1) month extension of time is hereby granted.

CONCLUSION

1. The patent owner's petition for extension for two (2) months time in which to file a response to the non-final Office action dated 19 January 2010 is hereby **granted-in-part**.
2. The period for response is extended by one (1) month.
3. The response is extended to **19 April 2010**.
4. All correspondence involving this proceeding may be addressed to the following:

By Mail to: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P. O. Box 1450
Alexandria, VA 22313-1450

By Fax to: (571) 273-9900
Central Reexamination Unit

By Hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

By EFS: Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at <https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html>. EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are “soft scanned” (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the “soft scanning” process is complete.

5. Telephone inquiries with regard to this decision should be directed to Mark Reinhart, at (571) 272-1611, in the absence of Mark Reinhart calls may be directed to Eric Keasel, at (571) 272-4929, or Jessica Harrison, at (571) 272-4449, all are Supervisory Patent Examiners in the Central Reexamination Unit, Art Unit 3992.

/Mark Reinhart/

Mark Reinhart,
Supervisory Patent Examiner,
AU 3992,
Central Reexamination Unit
571-272-1611

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)	
Edmund Munger, et al.)	
)	
U.S. Patent No.: 7,188,180)	
Filed: November 7, 2003)	Examiner:
Issued: March 6, 2007)	Andrew L. Nalven
)	
For: METHOD FOR ESTABLISHING)	Group Art Unit: 3992
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF)	
VIRTUAL PRIVATE NETWORK)	
)	
Reexamination Proceeding)	
Control No.: 95/001,270)	
Filed: December 8, 2009)	

NOTICE OF RECENT FILINGS IN CONCURRENT PATENT LITIGATION
PURSUANT TO 37 C.F.R. § 1.985 AND MPEP 2686

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. § 1.985 and MPEP 2686, the Patent Owner, VirnetX, Inc., notifies the Office of the filing of a Jury Verdict in *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-00080-LED, Dkt. No. 377 (E.D. Tex. March 16, 2010), attached hereto as Exhibit A, finding claims 1, 4, 15, 17, 20, 31, 33, and 35 of the above referenced patent valid and willfully infringed. The Patent Owner also notifies the Office of its filing of Plaintiff VirnetX Inc.'s Original Complaint in *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:10-cv-00094, Dkt. No. 1

Control Number: 95/001,270

(E.D. Tex. March 17, 2010), attached hereto as Exhibit B, which alleges infringement of the above referenced patent.

The commissioner is hereby authorized to charge any fees required 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

/Toby H. Kusmer/

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

Matthew E. Leno, Reg. No. 41,149

Hasan M. Rashid, Reg. No. 62,390

McDermott Will & Emery LLP

Attorneys for Applicant

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com
mleno@mwe.com
hrashid@mwe.com
Date: March 25, 2010

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
 Edmund Munger, et al.)
)
 U.S. Patent No.: 7,188,180)
 Filed: November 7, 2003) Examiner:
 Issued: March 6, 2007) Andrew L. Nalven
)
 For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
 SECURE COMMUNICATION LINK)
 BETWEEN COMPUTERS OF VIRTUAL)
 PRIVATE NETWORK)
)
 Reexamination Proceeding)
 Control No.: 95/001,270)
 Filed: December 8, 2009)

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the NOTICE OF RECENT FILINGS IN CONCURRENT PATENT LITIGATION PURSUANT TO 37 C.F.R. § 1.985 AND MPEP 2686, filed with United States Patent and Trademark Office on March 25, 2010, was served this 25th day of March, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Applicant

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

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: March 25, 2010
BST99 1646038-1.077580.0090

Electronic Acknowledgement Receipt

EFS ID:	7289172
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	25-MAR-2010
Filing Date:	08-DEC-2009
Time Stamp:	18:37:49
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notice of concurrent proceeding(s)	March25_Notice_Filings.pdf	32052 <small>4886a58f29fc0b5a5d834d31376759287945f356</small>	no	2

Warnings:

Information:

2	Reexam Certificate of Service	March25_CertServ.pdf	30772	no	1
			e31a0a73fb9da17b86c9f6021accdc01806d394e		
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	March_25EXA.pdf	324338	no	2
			d86e887af24f21888770587ceb78114d1103cf73		
Warnings:					
Information:					
4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	March_25EXB.pdf	127011	no	7
			e00d3ea19edca6c61e533d8e704a32a63505b8d		
Warnings:					
Information:					
Total Files Size (in bytes):				514173	

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

Re-Exam
Application
Control No. 95/001,270

Confirmation No. 2128

Based on U.S.
Patent No. 7,188,180
First Named
Inventor Victor Larson

Issued: 06/06/2007

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

Examiner: Andrew L. Nalven

Art Unit 3992

Mail Stop: Inter Partes Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

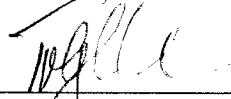
Enclosed for filing in connection with the above-referenced patent application are the following documents:

- 1) Information Disclosure Statement (2 pages)
- 2) Information Disclosure Statement by Applicant (Form 1449) (2 pages); and
- 3) Copies of references listed in the IDS Form 1449 (6 references).

There are no fees due with the filing of this Information Disclosure Statement. However, the Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

McDermott, Will & Emery LLP



Date: April 2, 2010

Toby H. Kusmer, Reg. No. 26,418
Atabak R. Royace, Reg. No. 59,037
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800

Docket No.: 077580-0090

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re-Exam

Application

Confirmation No. 2128

Control No. 95/001,270

Based on U.S.

Patent No. 7,188,180

Issued: 06/06/2007

First Named Inventor Victor Larson

Inventor

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

Examiner: Andrew L. Nalven

Art Unit 3992

Mail Stop: Inter Partes Reexam

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97, 1.98 and 1.555, 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 reexamination of the above-referenced patent, and that the documents be made of record therein and appear among the "References Cited" on any Re-examined patent to issue therefrom.

Although the undersigned attorney has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. The Examiner is invited to call the undersigned attorney for any questions regarding any of these documents.

This Statement is not to be interpreted as a representation that the cited publications are material, 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

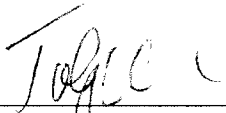
Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

The commissioner is hereby authorized to charge any fees required 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



Toby H. Kusmer, Reg. No. 26,418
Atabak R. Royae, Reg. No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800
Date: April 2, 2010

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

Subst. for form 1449/PTO

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

Complete if Known

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
	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	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
	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 4-Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	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

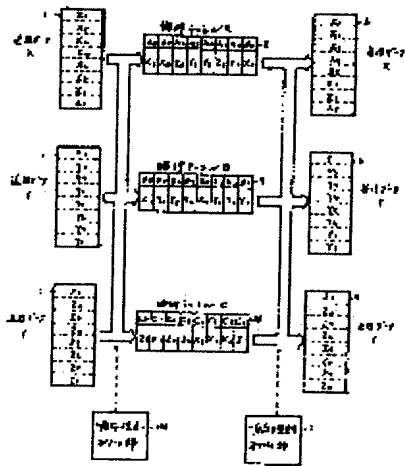
(11)Publication number : 62-214744

(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	1 0 2	B-7240-5K	昭和62年(1987)9月21日
11/20		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。

(従来の技術)

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並列させ、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のパケットデータに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

示す論理チャンネル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で示した論理チャンネル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。他の論理チャン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、複数の論理チャンネルを使用するため、各論理チャン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。

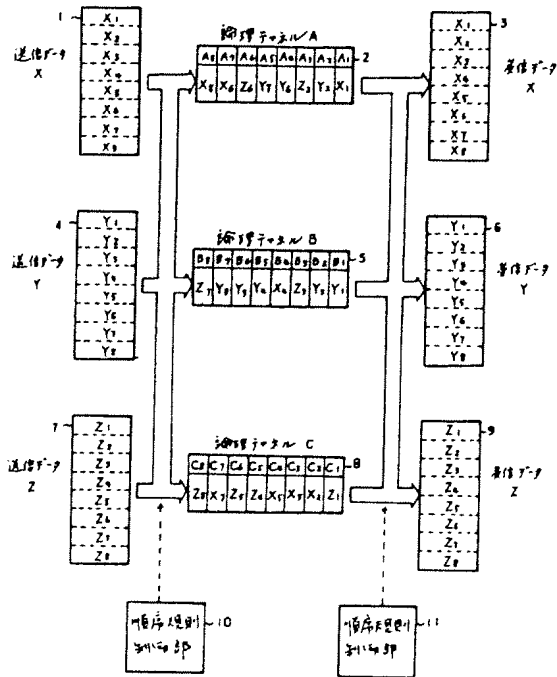
4. 図面の簡単な説明

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…論理チャンネル、
- 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

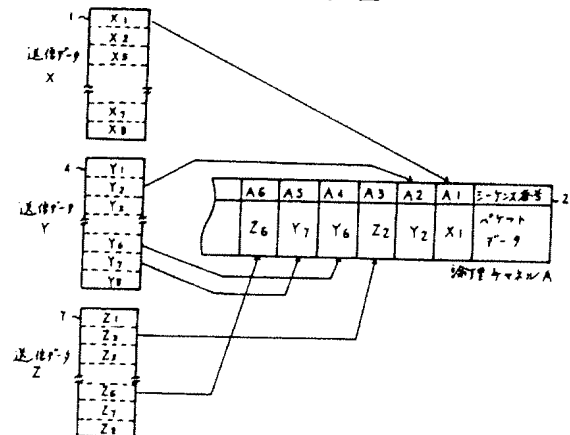
第1図



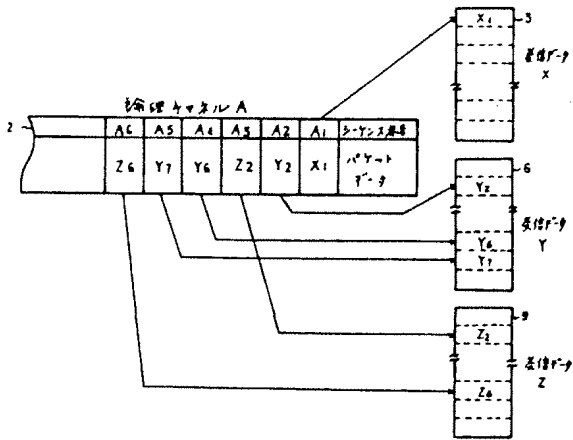
第2図

送信側順序規則	1	2	3	4	5	6	7	8	12
A	X_1	Y_2	Z_3	Y_4	Y_7	Z_6	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	

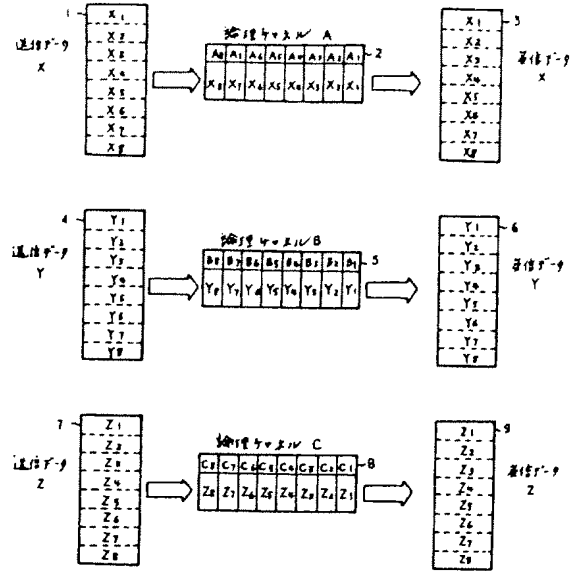
第3図



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

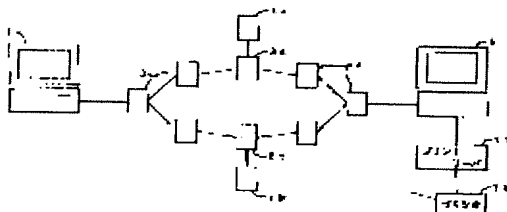
(21)Application number : 08-223898 (71)Applicant : BROTHER IND LTD
(22)Date of filing : 26.08.1996 (72)Inventor : SUZUKI MASASHI
MATSUDA KAZUHIKO
SAGOU AKIRA
KONDO HIROMOTO
YASUI TSUNEO

(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 SS21, S51, or 53, 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

(22) 出願日 平成8年(1996) 8月26日

(71) 出願人 000005267
 プ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

(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 プ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 プ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 プラザー工業株式会社内

(74) 代理人 弁理士 足立 勉

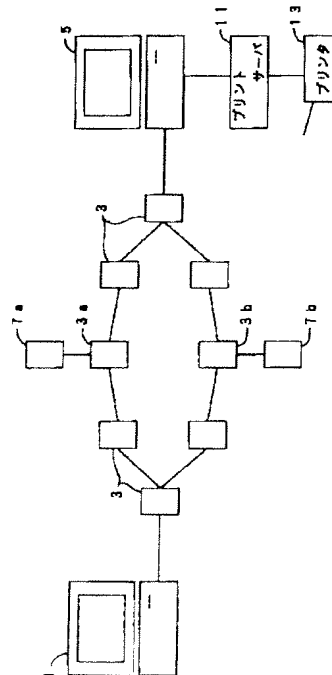
最終頁に続く

(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。

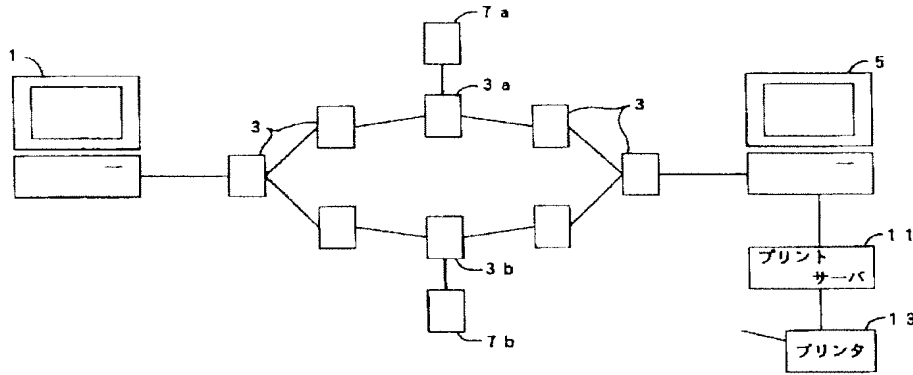
【図6】上記中継用サーバの処理の他の形態を表すフローチャートである。

【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。

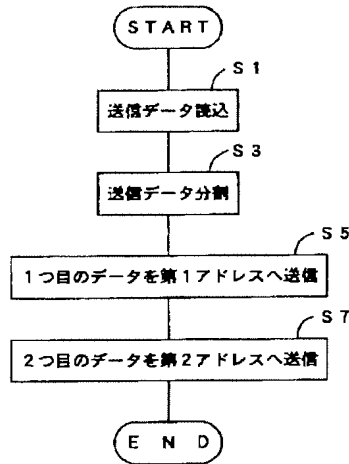
【符号の説明】

- 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

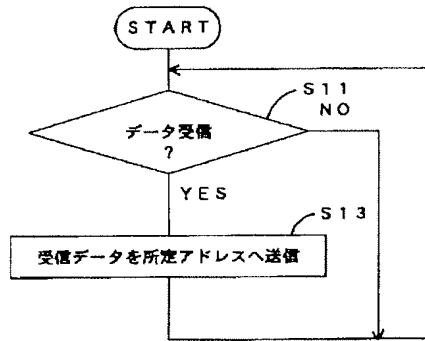
【図1】



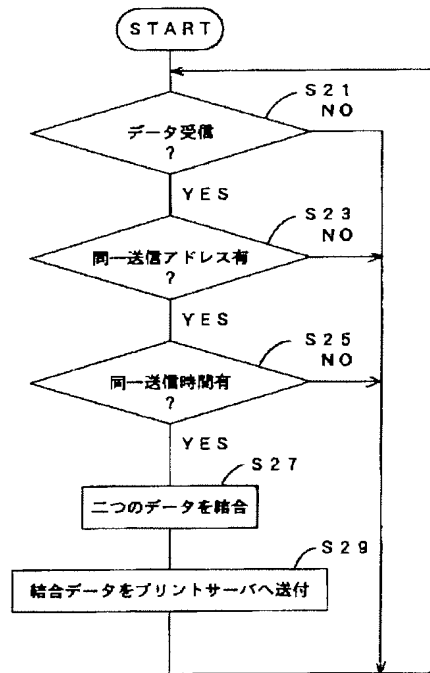
【図2】



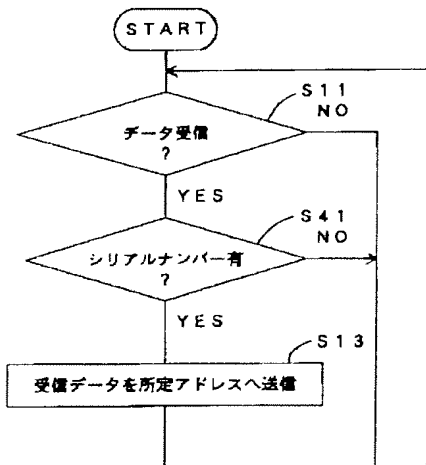
【図3】



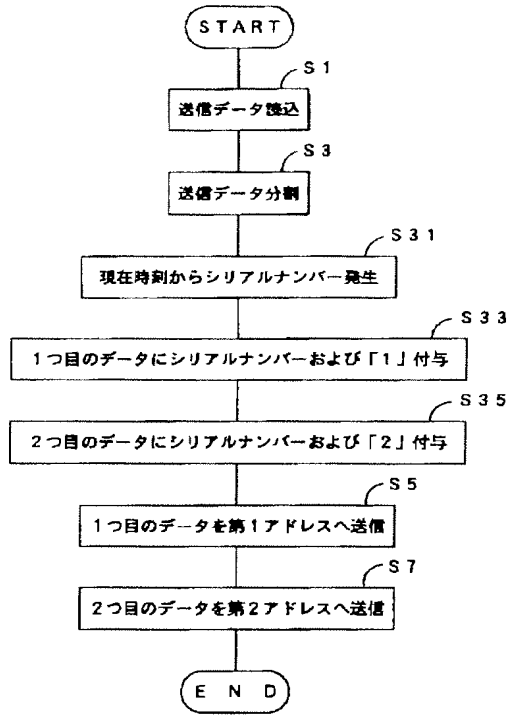
【図4】



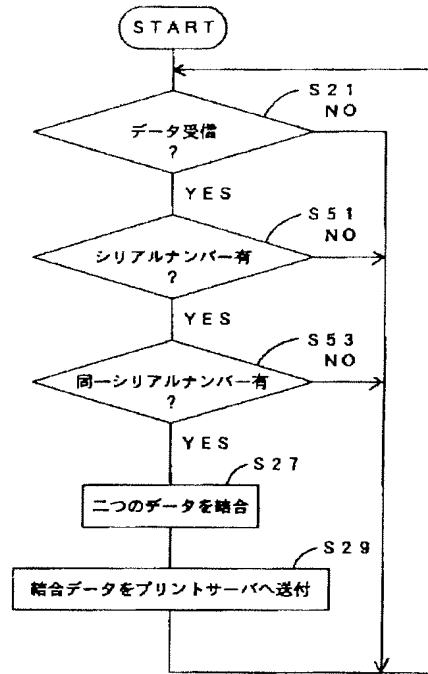
【図6】



【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

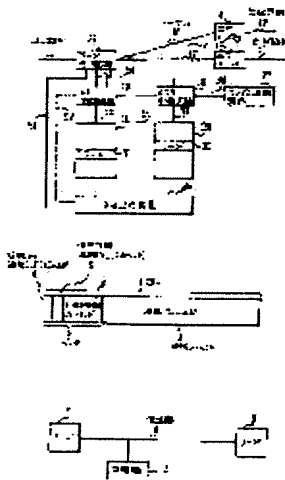
PATENT ABSTRACTS OF JAPAN

(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

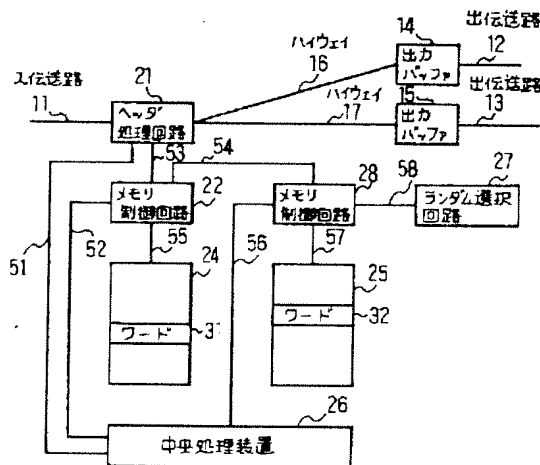
(74) 代理人 弁理士 並木 昭夫

(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。

20 【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りて説明する。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

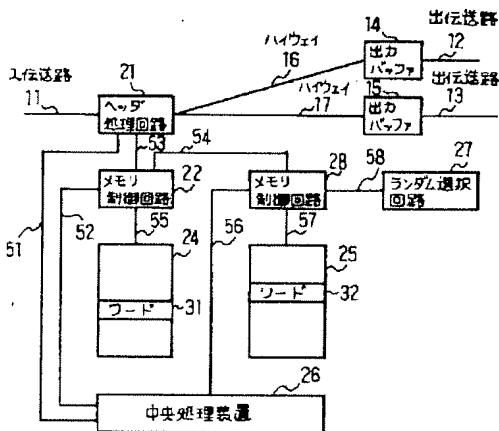
も図1と同様な構成で実現できることは明らかである。

【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。

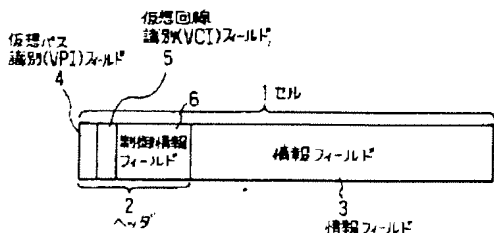
<1>

【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。

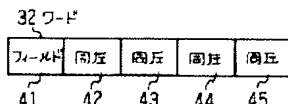
【図4】ノード間における盗聴の例を示すブロック図である。

<2>

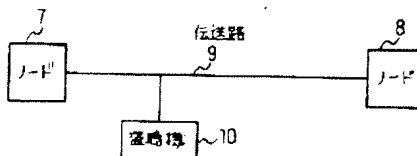
【符号の説明】

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

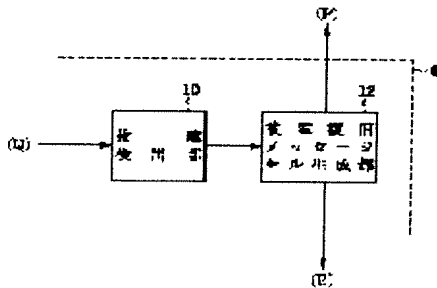
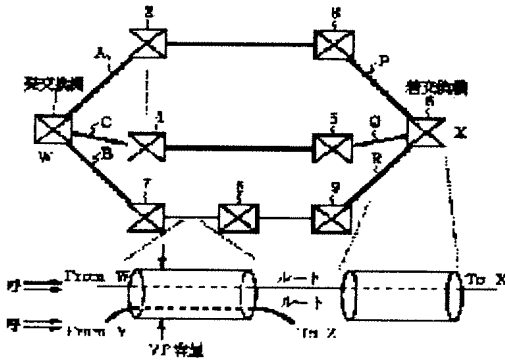
(11)Publication number : 09-018492

(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 hair drier (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	(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
(22) 出願日	平成7年(1995)6月30日	(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)

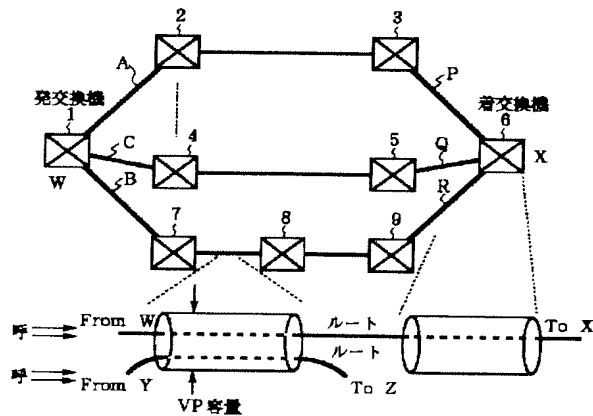
(54) 【発明の名称】 ATM通信網および故障復旧方法

(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、バスの接続先を記述したバス接続(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バ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バスを探索・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はバーチャルバスが設定される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、バーチャルバ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、バーチャルバ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、複数のバーチャルバ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バ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バスには現用のバーチャルバスおよび予備のバーチャルバスとなりうる複数のバーチャルバスがあらかじめ設定され、この現用のバーチャルバ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バスとなりうる複数のバーチャルバスにそれぞ

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し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、呼が受けられたら、VCコネクションを設定し、呼が受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ので、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。

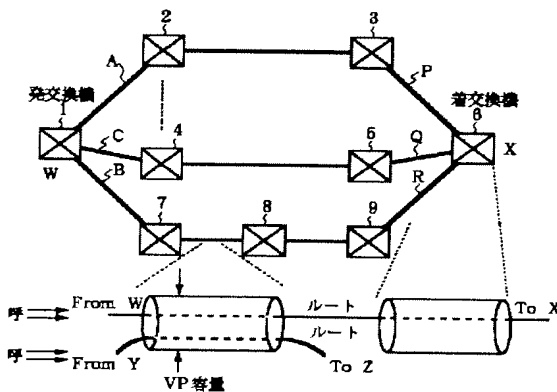
【図3】故障復旧メッセージセルの構成図。

【図4】中継交換機の要部ブロック構成図。

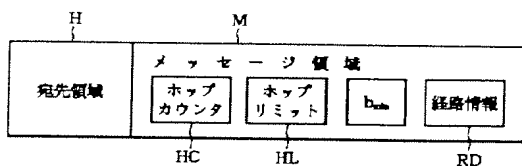
【図5】発交換機の要部ブロック構成図。

【図6】本発明第一実施例の動作を説明するための図。

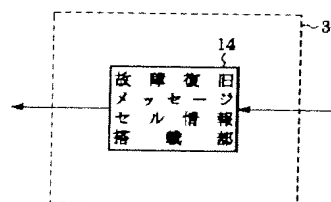
【図1】



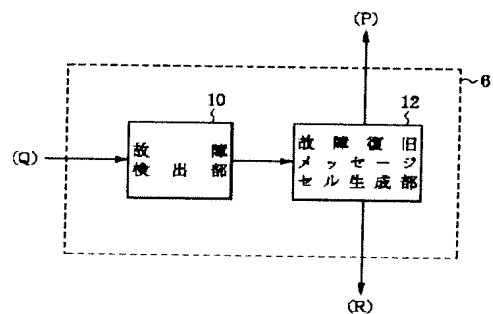
【図3】



【図4】



【図2】



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

20 HL ホップリミット

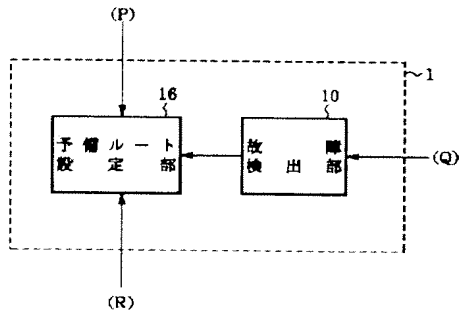
M メッセージ領域

RD 経路情報

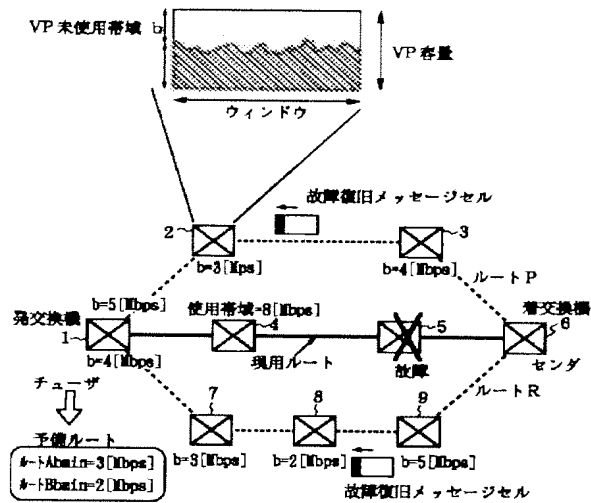
b_{min} 最小値

P、Q、R ルート

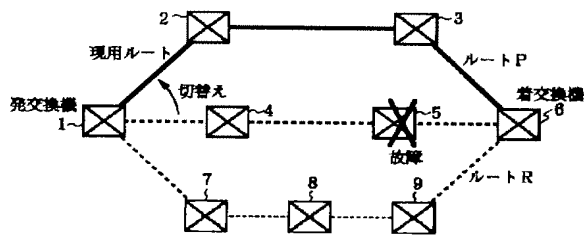
【図5】



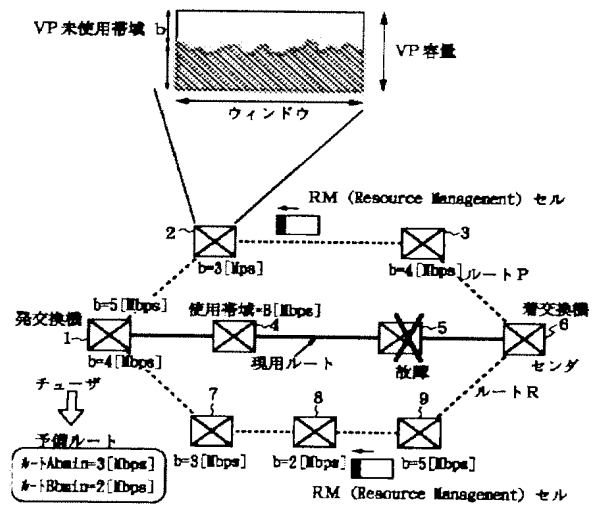
【図6】



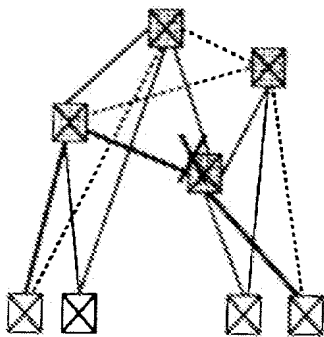
【図7】



【図8】

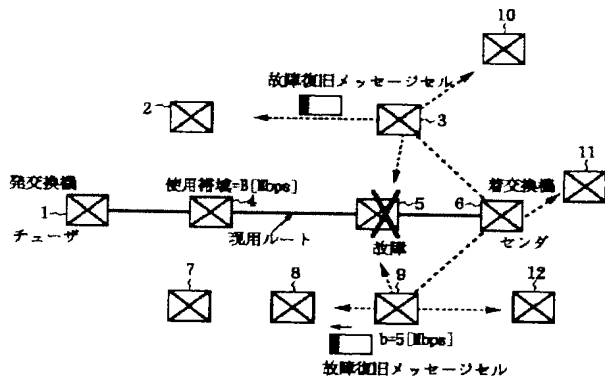


【図11】

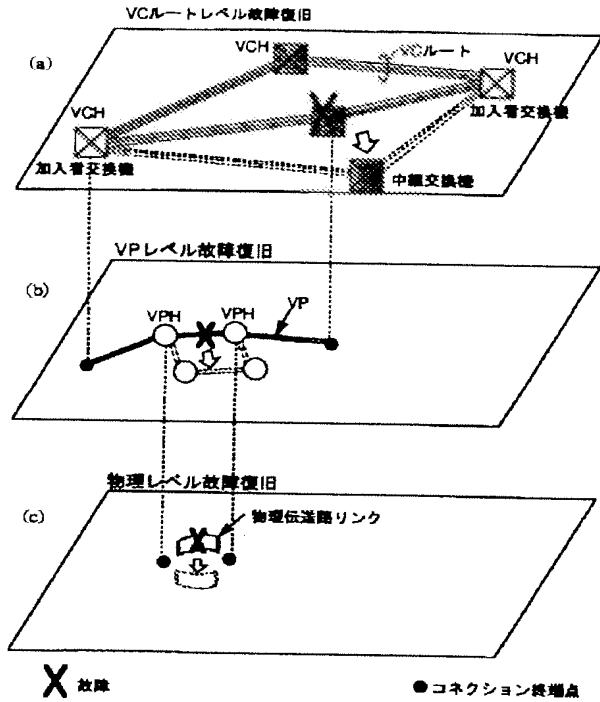


交換機のダウンサイジング化

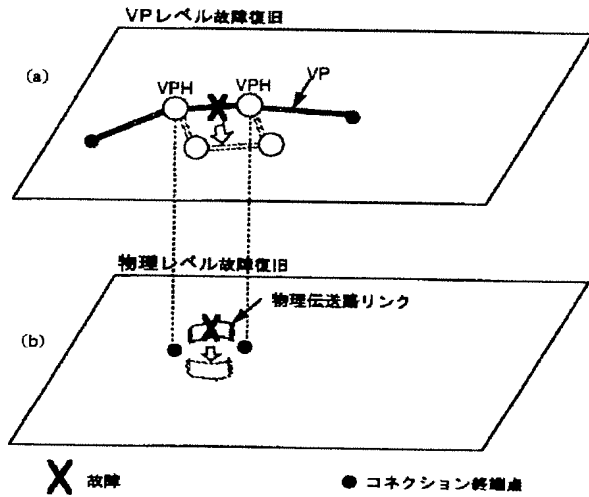
【図9】



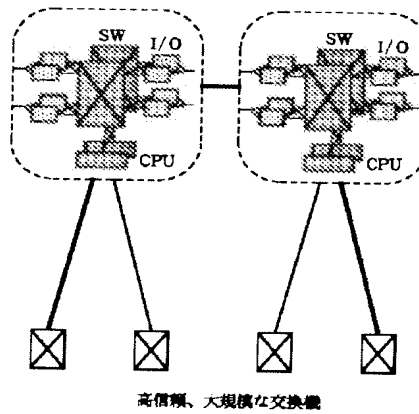
【図10】



【図12】



【図13】



Electronic Acknowledgement Receipt

EFS ID:	7342349
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Melissa Molchan
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	02-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	13:49:18
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		0090.pdf	125157 <small>96d76f06359e941a2afd2b44e7558cd45bb61cd8</small>	yes	7

Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Reexam Certificate of Service			1	1	
Information Disclosure Statement (IDS) Filed (SB/08)			2	7	
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	yes	53
			c1f5c3a6d9721eec83f8ef0087e759d448898a69		
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	Davies.pdf	572855	no	15
			570f1932ebcd625d840e44ae1e6c1c78603cf33c		
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	Feng.pdf	215626	no	4
			58bf05014b12aa13483ab383b6d7b0c529b2e711		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
Total Files Size (in bytes):			3073378		

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

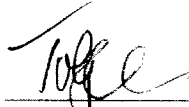
In the Reexamination of:)	
Victor Larson, et al.)	
)	
U.S. Patent No.: 7,188,180)	
Filed: November 7, 2003)	Examiner:
Issued: March 6, 2007)	Andrew L. Nalven
)	
For: METHOD FOR ESTABLISHING)	Group Art Unit: 3992
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF VIRTUAL)	
PRIVATE NETWORK)	
)	
Reexamination Proceeding)	
Control No.: 95/001,270)	
Filed: December 8, 2009)	

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Information Disclosure Statement, the Information Disclosure Citation, and references cited in the Information Disclosure Citation, which were filed with United States Patent and Trademark Office on April 2, 2010, were served this 2nd day of April, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP



Toby N. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Atabak R. Royae, Reg. No. 59,037
McDermott Will & Emery LLP
Attorneys for Patent Owner

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

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
Date: April 2, 2010

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
Edmund Munger, et al.)
)
U.S. Patent No.: 7,188,180)
Filed: November 7, 2003) Examiner:
Issued: March 6, 2007) Andrew L. Nalven
)
For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
SECURE COMMUNICATION LINK)
BETWEEN COMPUTERS OF)
VIRTUAL PRIVATE NETWORK)
)
Reexamination Proceeding)
Control No.: 95/001,270)
Filed: December 8, 2009)

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Declaration of Edmund Munger, Pursuant to 37 C.F.R. § 1.132, filed with United States Patent and Trademark Office on April 19, 2010, was served this 19th day of April, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Patent Owner
**Please recognize our Customer No. 23630 as
our correspondence address.**

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: April 19, 2010

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)	
Edmond Munger, et al.)	
)	
U.S. Patent No.: 7,188,180)	
Filed: November 7, 2003)	Examiner:
Issued: March 6, 2007)	Andrew L. Nalven
)	
For: METHOD FOR ESTABLISHING)	Group Art Unit: 3992
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF)	
VIRTUAL PRIVATE NETWORK)	
)	
Reexamination Proceeding)	
Control No.: 95/001,270)	
Filed: December 8, 2009)	

Declaration of Edmund Munger Pursuant to 37 C.F.R. § 1.132

Pursuant to 37 C.F.R. § 1.132, I, Edmund Munger, declare that the following statements are true to the best of my knowledge, information, and belief, formed after reasonable inquiry under the circumstances.

Background

1. I reside in Crownsville, Maryland. I have been the Chief Technology Officer of VirnetX, Inc. (“VirnetX”) since July 2006.
2. Prior to joining VirnetX Inc. from July 1987 to June 2006, I held various positions including Associate Division Manager, Division Manager, Chief System Architect and Assistant Vice President at Science Applications International Corporation (“SAIC”). Prior to SAIC, I was the chief system architect for the FBI’s Counterterrorism Data Warehouse Prototype, and have worked on several advanced defense systems. I received a M.S. in Naval Architecture and Marine Engineering from MIT and a B.S. in Naval Science from the United States Naval Academy.
3. I am one of the named inventors of U.S. Patent No. 7,188,180 (the “‘180 Patent”) which is the subject of the above identified reexamination proceeding. I am very familiar with the ‘180 Patent, including all of the claims of the patent, claims 1-41.

4. On March 16, 2010, claims 1, 4, 15, 17, 20, 31, 33 and 35 of the '180 Patent were found to be not invalid and to be willfully infringed by Microsoft Corporation in the matter of *VirnetX, Inc. v. Microsoft Corporation*, United States District Court For The Eastern District Of Texas, Case No. 6:07 cv 80. The jury in that case awarded VirnetX thirty four millions dollars (\$34,000,000) in damages for such infringement.¹

5. Prior to and at the time of the claimed invention as defined by at least claims 1, 17 and 33 of the '180 Patent, there was a significant and increasing concern with the security of computer communication. The widespread connectivity between computers that was enabled by the swift increase in network access in homes and businesses also led to many security breaches as well as concerns regarding the safety of confidential data sent over computer networks. This problem received significant attention from the research and development community. Practical experience showed that there was a need for a system that could be easily and correctly used. In August 1998 I published an article describing such need. A solution that was difficult for an end-user to employ would likely have led to a lack of use or incorrect use. I believe that the invention defined by at least claims 1, 17 and 33 of the '180 Patent (all of which are under reexamination) has met that criteria.

6. As one example of the manifestation of this need, the Defense Advanced Research Projects Agency ("DARPA"), funded various research programs to further the science and technology of information assurance and survivability. DARPA programs, such as "Information Assurance" and "Dynamic Coalitions" were focused on the long-felt need to provide easy-to-use secure communications. These projects received significant funding to be spent developing technologies that could solve this need. For example, one such project entitled "Next Generation Internet" received funding in fiscal year 1998 of approximately \$39.3 Million, in fiscal year 1999 of approximately \$49.5 Million and in fiscal year 2000 of approximately \$40 Million.² Another program funded by DARPA, "Dynamic Coalitions," was created to address the ability of the Department of Defense to quickly and easily set-up secure communications over the Internet.

¹ I have been informed that a copy of the verdict awarding these damages was submitted to the Patent Office on March 25, 2010 as Exhibit A to Notice Of Recent Filings In Concurrent Patent Litigation Pursuant To 37 C.F.R. §1.985 And MPEP 2686.

² See, e.g., Exhibit A.

7. According to DARPA officials at the time, “existing group membership protocols did not support the security needs of multidimensional organizations.”³ The overarching challenge is to create secure groups rapidly. This is a significant issue when countries are faced with an operation that requires immediate multinational attention.”⁴ DARPA contracted with some of the most skilled organizations in the area of secured communications in an effort to meet its security needs (e.g., NAI Labs, a division of PGP Security, Network Associates Incorporated, Los Angeles, and the Microelectronics Center of North Carolina, Research Triangle Park, North Carolina, as well as Johns Hopkins University, Baltimore; Northeastern University, Boston; and Veridian-PSR, Arlington, Virginia). In all, more than 15 organizations are researching the various components that make up the program initiated by the Department of Defense.⁵ However, none of these prestigious institutions came up with a solution, at the relevant time frame, close to solution provided by the claimed invention as defined by at least claims 1, 17 and 33 of the ’180 Patent.⁶

8. As a second example, In-Q-Tel, a company with strong ties to the United States Central Intelligence Agency (“CIA”), funded the original development of technology relating to secure remote connections with approximately \$3.4 Million.

9. SAIC’s business model is to sell hours to the federal government. SAIC is not designed to bring products to the market, which typically make significant internal investments in research and development. In an average year during the development of the claimed invention as defined by at least claims 1, 17 and 33 of the ’180 Patent, SAIC would spend approximately \$2 million on internal research and development efforts. In the case of developing a secure remote connection technology, SAIC invested \$1.7 million, which represents almost the entirety of SAIC’s internal research and development budget for one whole year. A technology review committee also approved the team’s patent development efforts and costs on an ongoing basis. A third party (Cambridge Research Group) also substantiated the value of the technology. Moreover, a significant percentage of all of SAIC’s patent development efforts have focused on this technology. I was told that their patent portfolio was 1/3 of SAIC’s patent portfolio efforts at that time.

³ Exhibit B.

⁴ Exhibit C.

⁵ See e.g., Exhibit D.

10. In fact, in 1998, before the claimed invention of the '180 Patent, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks.⁷ At that time period, remote access was “a nightmare for support desks. Staffers never know what combination of CPU, modem, operating system and software configuration they’re going to have to support” and adding the commercially available VPN software only made matters worse. Further, this article precisely captured the computer and internet security industry’s attitude toward the tradeoff between the ease of use of a VPN system for the average computer user and the security that the VPN system provided. The article recognized that the “ease of installation isn’t always a good thing: In many cases, the easier the client is to install, the less secure it is.” However the claimed invention as defined by at least claims 1, 17 and 33 of the '180 Patent, combine both the ease of use and security aspects of a VPN without sacrificing one or the other.

11. Further, it was not until 2004, well after the filing of the application that matured into the '180 Patent, that Microsoft started to advertise for an increasingly sophisticated security landscape.⁸ Mr. Gates in this article discussed how “Microsoft is taking steps toward making computers more resilient in the presence of worms and viruses, enabling customers to communicate and collaborate in a more secure manner. Microsoft is focusing on the development of technologies designed to make this vision a reality and extend protection to PCs themselves. “No single technology can adequately protect against the many different kinds of attacks that computers face,” Gates said. “Resiliency can only be achieved with a combination of security technologies designed to combat the sophisticated threat from worms and viruses.. ..Our strategy has been, and continues to be, to make security a built-in piece of everything we provide, not a bolt-on,” said Jim McDonnell, vice president of worldwide marketing at HP. As part of that commitment, HP is pleased to bring our customers these additional security enhancements through Microsoft Windows XP SP2.”⁹

12. VirnetX and its predecessor in interest, SAIC, were able to attract interest in the secure remote connection technology being developed. In particular, SafeNet, a leading provider of Internet security technology that is the de facto standard in the VPN industry and entered into a

⁶ Id.

⁷ See, e.g., Exhibit E.

⁸ Exhibit F.

portfolio license with SAIC on July 2002 to incorporate the features into SafeNet's underlying VPNs.

13. At the time of the claimed invention as defined by at least claims 1, 17 and 33 of the '180 Patent, there was a significant focus on IETF protocols, including IPsec and various VPN technologies. Although there was significant research and publication on these topics, no one suggested the use of DNS queries to trigger VPNs. Moreover, there was a general understanding that security could only be achieved through difficult-to-provision and create VPNs. On the other hand, the general consensus was that easy-to-set-up connections could not be secure. This belief was reinforced by the IT offices of many large companies and institutions, whose livelihood depended on the need for highly trained specialists to arrange secure network connections.

14. I hereby declare that all statements made herein of my own knowledge are true and that

⁹ Id. See also, Exhibit G.

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.

Date: April 14, 2010


Edmund Munger

BST99 1647665-2.077580.0090

Electronic Acknowledgement Receipt

EFS ID:	7444307
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	19-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	18:56:27
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Certificate of Service	Cert_Serv_Munger.pdf	24103 <small>207b90b01a2a776a4ed372da06fe3600829b8773</small>	no	1

Warnings:

Information:

2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Munger_Declaration.pdf	70185	no	6
			87cd14d81895c15602b4136a28c2f78cb16084e7		
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_a_part_1.pdf	16107594	no	113
			131bb6cb430bc496bd69bd010faa4273aba9ed06		
Warnings:					
Information:					
4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_a_part_2.pdf	23032070	no	107
			3d867f222cf97ecc4051aa3f2a36882b3a81f3bc		
Warnings:					
Information:					
5	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_a_part_3.pdf	14641746	no	64
			b826668b1afb5c387e913227f1fc42035ddeeb06		
Warnings:					
Information:					
6	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_b_part_2.pdf	21437136	no	22
			60ab52a3e3ec5b43df723c2c51f660d4bebc804		
Warnings:					
Information:					
7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_b_part_1.pdf	9322017	no	60
			10969bfdca79ed8a9aedf54a343fabf5129a123f		
Warnings:					
Information:					
8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Exhibit_C.pdf	13155708	no	52
			88e5d5735de5ced96c5ae29e4317b5f82075adce		
Warnings:					
Information:					
9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Exhibit_D.pdf	1167728	no	5
			b3630958be906eeb2fb686a9bc22794878a182af		
Warnings:					
Information:					
10	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_e_part_1.pdf	24008441	no	151
			a23d4b6dfa3ca47de3cc5f59af39f0620cc76e8		
Warnings:					
Information:					

11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_e_part_2.pdf	23996879 fa6a613b56aae2628f5bed042239d22070150967	no	94
Warnings:					
Information:					
12	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_e_part_3.pdf	19490999 9f6006bd6fae80115a557b9dd8102f35450a5e6d	no	68
Warnings:					
Information:					
13	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	exhibit_e_part_4.pdf	12140393 e98a10a8cf1c7c8e75174b2f872b698cb26878a7	no	61
Warnings:					
Information:					
14	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Exhibit_F.pdf	275647 927f10fd866b7d9a38deb90289ff35083f2eed2d	no	5
Warnings:					
Information:					
15	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Exhibit_G.pdf	27608 b44674c17fd9b3b757a4a214113f4945b0959fb4	no	7
Warnings:					
Information:					
Total Files Size (in bytes):			178898254		

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 the Reexamination of:)	
Edmund Munger, et al.)	
)	
U.S. Patent No.: 7,188,180)	
Filed: November 7, 2003)	Examiner:
Issued: March 6, 2007)	Andrew L. Nalven
)	
For: METHOD FOR ESTABLISHING)	Group Art Unit: 3992
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF)	
VIRTUAL PRIVATE NETWORK)	
)	
Reexamination Proceeding)	
Control No.: 95/001,270)	
Filed: December 8, 2009)	

RESPONSE TO OFFICE ACTION IN REEXAMINATION

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Patent Owner hereby responds to the Office Action dated January 19, 2010 (“the Office Action”) in the Reexamination of the above-mentioned patent (“the ‘180 Patent”) having a period of response set to expire on April 19, 2010 in view of the extension of time granted on February 25, 2010.

Remarks begin on page 2 of this response.

REMARKS

Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 Patent are under reexamination, with claims 1, 17, and 33 being independent. Claims 1, 10, 12-15, 17, 26, 28-31, and 33 stand rejected. Claims 4, 20, and 35 are confirmed to be patentable.

Submitted herewith is a Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132 ("Nieh Dec.") in support of the Patent Owner's response.

I. Patent Owner's Response To the Rejection

A. Introduction

The Patent Owner's invention, as defined in independent claim 1, is directed to a method for accessing a secure computer network address. The method comprises the steps of: (i) receiving a secure domain name; (ii) sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name; (iii) receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and (iv) sending an access request message to the secure computer network address using a virtual private network communication link.

The patent provides a technique for establishing a virtual private network ("VPN") communication link between a first computer and a second computer over a computer network. '180 Patent at col. 49, ll. 57-59. To illustrate one non-limiting example, a client computer is connected to a computer network, such as the Internet. *Id.* at col. 50, ll. 1-4. The client computer connects to a server over a non-VPN communication link using a web browser to display a web page. *Id.* at col. 50, ll. 8-25.

According to one variation, the web page can contain a hyperlink for selecting a VPN communication link to the server. *Id.* at col. 50, ll. 25-31. By selecting the hyperlink, a client can secure the communication between itself and the server. *Id.* at col. 51, ll. 5-14. The user need only click the hyperlink – no need to enter user identification information, passwords, or encryption keys. *Id.* Accordingly, in this example, establishing a secure communication link between the user and server are performed transparently to a user. *Id.* To support this transparency, the technique disclosed in the '180 Patent provides for automatically replacing the

Control Number: 95/001,270

top-level domain name of the server within the web browser with a secure top-level domain name for the server. *Id.* at col. 51, ll. 15-28. For example, if the top-level domain name for the server is “.com,” it may be replaced with “.scom”. *Id.*

Because a secure top-level domain name can be a non-standard domain name, a query to a standard domain name system (“DNS”) would return a message indicating that the universal resource locator (“URL”) is unknown. *Id.* at col. 51, ll. 28-35. Therefore, according to the patent, the query can be sent to a secure domain name service for obtaining the URL for the secure top-level domain name. *Id.* The secure domain name service can contain a cross-reference database of secure domain names and corresponding secure network addresses. *Id.* at col. 52, ll. 4-26. That is, for each secure domain name, the secure domain name service stores a computer network address corresponding to the secure domain name. *Id.* An entity can register a secure domain name in the secure domain name service so that a user who desires a secure communication link to the web site of the entity can automatically obtain the secure computer network address for the secure website. *Id.* An entity can also register several secure domain names, with each respective secure domain name representing a different priority level of access to the secure website. *Id.*

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. *Id.* 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. *Id.* When a user queries the secure domain name service for the secure computer network address for the securities trading website, the secure domain name service determines the particular secure computer network address based on the user's identity and the user's subscription level. *Id.*

B. Applicable Standards for Rejection

1. Applicable Standard for Rejection Under 35 U.S.C. § 102

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102. A rejection under 35 U.S.C. § 102 requires that “each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *See* MPEP § 2131, citing *Verdegaal Bros. v. Union Oil Col. of California*, 814 F.2d

628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The above-stated rejection, however, fails to meet this standard.

2. Applicable Standard for Rejection Under 35 U.S.C. § 103(a)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent also stand rejected under 35 U.S.C. § 103(a). In reconsidering the outstanding 35 U.S.C. § 103(a) rejections, the Examiner must consider any evidence supporting the patentability of the claimed invention, such as any evidence in the specification or any other evidence submitted by the Patent Owner, such as the secondary considerations of non-obviousness submitted herewith. The ultimate determination of patentability is based on the entire record, by a preponderance of evidence, which requires the evidence to be more convincing than the evidence which is sought in opposition to it. *See* MPEP § 2142 (citing *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992)).

Each of the rejections under 35 U.S.C. § 103(a) fails to meet these standards by a preponderance of the evidence.

3. Applicable Standard for Demonstrating a Publication Date

As identified below, a number of references have not been shown to qualify as prior art to the '180 Patent. The Office Action and the Request for *Inter Partes* Reexamination of Patent ("Request") both fail to demonstrate the actual publication date of various of the relied upon references necessary to establish a *prima facie* showing that each reference is prior art. The Patent Owner is left to assume that the assertion that the references are prior art arises from the copyright date printed on the face of each reference. This copyright date is not, however, the 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, 226 (C.C.P.A. 1981). Unlike a publication date, a copyright date merely establishes "the date that the document was created or printed." *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 975 (E.D. Mich. 2003).

Presuming the author of a document accurately represented the date the document was created, this creation date is not evidence of any sort of publication or dissemination. Without

more, a 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.

The party asserting the prior art bears the burden of establishing a date of publication. *See Carella v. Starlight Archery*, 804 F.2d 135, 139 (Fed. Cir. 1986) (finding that a mailer did not qualify as prior art because there was no evidence as to when the mailer was received by any of the addresses). Here, the Office bears the burden of establishing a prima facie case of unapertability, including that the references relied upon are proper prior art. *See In re Hall*, 781 F.2d 897 (Fed. Cir. 1986)(Affidavits on public availability of a reference were necessary for the Examiner to establish the reference to be prior art.). Yet, neither the Office Action nor the Request even attempt to show that various of the references identified below were disseminated or made publicly available.

Thus, the Patent Owner respectfully submits that, as demonstrated below, a number of references relied upon in the Office Action have not been shown to be prior art to the rejected claims. Accordingly, the Patent Owner respectfully requests that the rejections over these references be withdrawn.

C. The Rejection of Claims Over Alleged Prior Art

The outstanding rejections rely on the erroneous premise that the “secure domain name” and “secure domain name service” recited in independent claims 1, 17, and 33 of the ‘180 Patent are a standard domain name and domain name service, respectively. In the interest of brevity, the Patent Owner here reveals the fault in this premise by outlining the differences here at the outset and refers back to these statements when addressing each rejection of the Office Action below.

The Request and Office Action rely on the erroneous premise that a secure domain name is a domain name that happens to correspond to a secure computer. *See, e.g.*, Office Action at 6; Request at 15. Alternatively, the Request and Office Action rely on the faulty position that a secure domain name corresponds to an address that simply requires authorization. Request at 21. These assertions are in clear contradiction to the specification of the ‘180 Patent, which takes pains to explain that a secure domain name is different from a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization. *Id.*; ‘180 Patent at col. 51, ll. 18-28; Nieh Dec. at ¶ 10. To illustrate, in various

implementations, the '180 Patent describes that a secure domain name is a "a non-standard domain name." '180 Patent at col. 51, ll. 29-31; Nieh Dec. at ¶ 10. Examples of such non-standard domain names are described in Claim 11: .scom, .snet, .sorg, .sedu, .smil, and .sgov. Nieh Dec. at ¶ 10. Dependent claim 2 also differentiates between a secure domain name and a non-secure domain name in reciting the step of "automatically generating a secure domain name corresponding to a non-secure domain name." *Id.* To further illustrate, the '180 Patent describes that "a query [with a secure domain name] to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." *Id.*; '180 Patent at col. 51, ll. 28-32. Thus, the Patent Owner respectfully submits that the inventors of the '180 Patent acted as their own lexicographers in providing that the secure domain name recited in claims 1, 17, and 33 of the '180 Patent cannot be properly read to be a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization. Nieh Dec. at ¶ 10. As seen from the previous sentences, a secure domain name is different from a domain name that just happens to be associated with a secure computer or secure computer network address. For example, as pointed above, the domain name that just happens to correspond to a secure computer or a domain name that just happens to correspond to an address requiring authentication can be resolved, for example, by a conventional domain name service; whereas, as noted above, a secure domain name cannot be resolved by a conventional domain name service, for example. *Id.*

Furthermore, the Patent Owner notes that even if the recitation "secure domain name" is defined according to the Request to mean a domain name corresponding to a secure computer or a domain name corresponding to an address requiring authorization, various of the cited documents still fail to describe or suggest this feature. Nieh Dec. at ¶ 11. Specifically, the relied upon portions of the cited documents describe domain names of computers that do not require authorization for access. Instead, the computers (*e.g.*, a VPN tunnel server or a PPTP server) of the cited documents are for securing a connection between a client computer and a target computer. *Id.* To this end, the computers (*e.g.*, a VPN tunnel server or a PPTP server) themselves do not have a secure computer network address because they do not require authorization for access or authorization for a client computer to communicate with them. *Id.* Any client computer can without authorization communicate with one of these computers (*e.g.* a VPN tunnel server or a PPTP server); it is the target computer that may requires authorization for

access. *Id.* Therefore, neither the domain name of the computers (*e.g.*, a VPN tunnel server or a PPTP server) nor their corresponding computer network address is secure – even if this term is defined according to the Request. *Id.* As such, these cited documents do not teach a secure computer network address or, correspondingly, a secure domain name.

Similarly, the Request and Office Action rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of secure computers. *See, e.g.*, Office Action at 7; Request at 15. Alternatively, the Request and Office Action also rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of computers that are used to establish a secure connection, such as a VPN tunnel server or a PPTP server. *See, e.g.*, Office Action at 16; Request at 21. Again, these arguments are belied by the ‘180 Patent itself. The specification of the ‘180 Patent clearly teaches that the claimed secure domain name service is unlike a conventional domain name service, which the inventors understood as including both DNS and DNS with public key security. Nieh Dec. at ¶ 12; *see col. 51, ll. 29-45; col. 52, ll. 4-26.* To illustrate, the ‘180 Patent explicitly states 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. *See, ‘180 Patent at col. 51, ll. 18-45* (stating “[b]ecause 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”); Nieh Dec. at ¶ 12. A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name. Nieh Dec. at ¶ 12. A secure domain name service of the ‘180 Patent, instead, recognizes that a query message is requesting a secure computer network address and performs its services accordingly. Nieh Dec. at ¶ 12. Furthermore, in various implementations, the ‘180 Patent describes a secure domain name service as providing additional functionalities not available with a traditional domain name service, as described above in Section I.A. and in the ‘180 Patent at col. 52, ll. 4-26. *Id.* The ‘180 Patent even describes the drawbacks of the conventional scheme of traditional DNS and public key security:

One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve

automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).

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

‘180 Patent at col. 40, ll. 6-17; Nieh Dec. at ¶ 12. Thus, the Patent Owner respectfully submits that the secure domain name service recited in claims 1, 17, and 33 of the ‘180 Patent is different from a conventional domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

1. The Rejection of Claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 Under 35 U.S.C. § 102(a) in view of Aventail Connect v3.1/v2.6 Administrator’s Guide (hereafter “Aventail”)

Claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Aventail. The rejection is based on the reasons given on pages 12-19 of the Request, Appendix A to the Request, and the additional reasons presented on pages 6-12 of the Office Action. The Patent Owner respectfully traverses this rejection because (i) Aventail has not been shown to be prior art under § 102(a) and (ii) assuming, *arguendo*, that Aventail qualifies as prior art, Aventail has not been shown to teach, either expressly or inherently, each and every element of independent claims 1, 17, and 33. The following remarks address each of these points in turn.

a) Aventail has not been shown to be prior art under § 102(a)

Both the Office Action and the Request assert that Aventail was published between 1996 and 1999 without any stated support. Request at 5; Office Action at 2. The Patent Owner can only presume that this assertion arises from the copyright date range printed on the face of the reference: “© 1996-1999 Aventail Corporation.” See Aventail at *i*. As stated in Section I.B.3., above, this copyright date range is not the publication date of Aventail and the Office Action has failed to make any showing that it is.

Further, the closeness of proximity of the alleged publication date of Aventail to the April 26, 2000 priority date of the ‘180 Patent raises further doubt as to the availability of Aventail as prior art. Suppose the relied upon sections of the Aventail reference were created on December

31, 1999, and the copyright date range accordingly amended to read “1996-1999.” Under these circumstances, it is possible that the document was not disseminated until after the filing date of the ‘180 Patent, a mere four months later. Under these circumstances, Aventail clearly would not be eligible to be relied upon as prior art to the ‘180 Patent.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Aventail is prior art and requests all rejections based on Aventail be withdrawn. Nonetheless, the Patent Owner addresses Aventail below as though it is qualified prior art.

b) Aventail has not been shown to teach each and every element of independent claims 1, 17, and 33

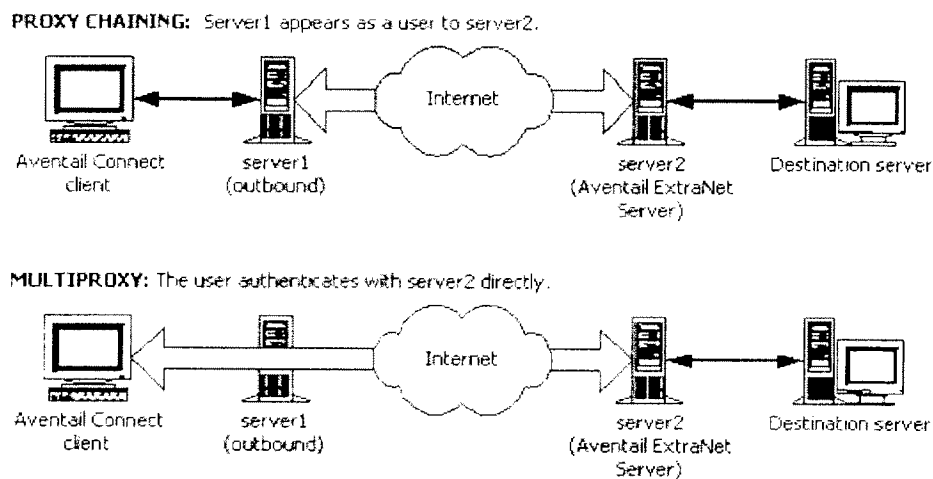
(1) Aventail fails to teach “a secure domain name” and “a secure domain name service”

First, Aventail fails to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Aventail discloses a system and architecture for transmitting data between two computers using the SOCKS protocol. Nieh Dec. 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 Dec. at ¶ 14. Upon receipt of the network traffic, the SOCKS server transmits the network traffic to the Internet or external network. Aventail at 7; Nieh Dec. at ¶ 14. Aventail’s disclosure is limited to connections created at the socket layer of the network architecture. Nieh Dec. at ¶ 14.

In operation, Aventail discloses that a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. Aventail at 9; Nieh Dec. at ¶ 15. The Aventail Connect software is disclosed to intercept 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 Dec. 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 Dec. 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 Dec. at ¶ 16. The SOCKS server performs the hostname resolution. Aventail at 12; Nieh Dec. at ¶ 17. Once the hostname is resolved, the user can transmit data over

a SOCKS connection to the SOCKS server. Nieh Dec. at ¶ 17. The SOCKS server, then, separately relays that transmitted data to the target. *Id.*

Along with this basic operation, the Request cites to a “Proxy Chaining” and a “MultiProxy” mode disclosed in Aventail. Request at 12; Aventail at 68-73. In the “Proxy Chaining” mode, Aventail discloses that a user can communicate with a target via a number of proxies such that each proxy server acts as a client to the next downstream proxy server. Aventail at 68; Nieh Dec. at ¶ 18. As shown below, in this mode, the user does not communicate directly with the proxy servers other than the one immediately downstream from it. Aventail at 68, 72; Nieh Dec. at ¶ 18.



Aventail at 72. In the “MultiProxy” mode, Aventail discloses that the user, via Aventail Connect, connects through each successive proxy server directly. Aventail at 68; Nieh Dec. at ¶ 20. Regardless of whether one of these modes is enabled, the operation of Aventail Connect does not materially differ between the methods. Nieh Dec. at ¶ 21.

Nowhere in these teachings does Aventail teach a secure domain name. The Office Action asserts that the hostname (e.g., the alleged secure domain name) is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption. Office Action at 6. To this end, the Office Action interprets a secure domain name as a domain name associated with a secure computer. *Id.* As stated above at the beginning of Section I.C., which is incorporated herein by reference, this assertion is incorrect. *See also* Nieh Dec. at ¶ 22.

Similarly, Aventail has not been shown to teach a secure domain name service. The Office Action suggests that a DNS server that can resolve addresses of secure computers

corresponds to a secure domain name service. *See*, Office Action at 7. This is incorrect. Aventail has not been shown to teach anything more than a conventional DNS. Nieh Dec. at ¶ 23. As stated above in the beginning of Section I.C., a secure domain name service is not a conventional domain name service. *Id.* A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

The Request has not shown Aventail to disclose a domain name service other than a traditional domain name service. The Request asserts that Aventail discloses two look-up services, alleged to be described on pages 8 and 12 of that reference. Request at 15. On page 8, Aventail discloses the traditional protocol for a computer to connect to a remote host. Nieh Dec. at ¶ 24. On page 12, Aventail discloses “forward[ing] the host-name to the extranet (SOCKS) server [where] the SOCKS server performs the hostname resolution.” *Id.* Thus, Aventail has not been shown to disclose anything other than a traditional DNS. *Id.* As noted above at the outset of Section I.C., a secure domain name service is unlike a conventional domain name service. *Id.* A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

For at least these reason, Aventail fails to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of independent claims 1, 17, and 33 and the rejected dependent claims 10, 12, 14, 26, 28, 30, and 31.

(2) Aventail fails to teach “a virtual private network link”

Aventail has not been shown to teach sending an access request message to a secure computer network address using a virtual private *network* communication link, as recited in claims 1, 17, and 33.

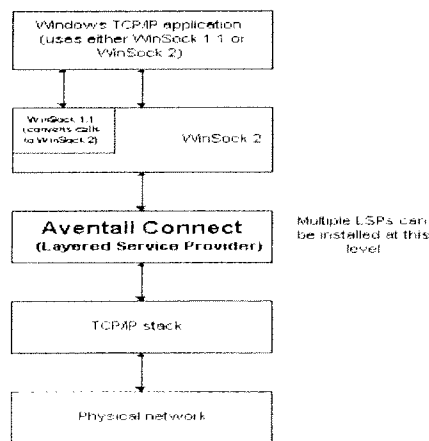
The links created by the systems and methods disclosed in Aventail differ from the virtual private network communication link recited in claims 1, 17, and 33. Nieh Dec. at ¶ 25. First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network. *Id.* 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 virtual private network, as recited in claims 1, 17, and 33, 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 virtual private network. *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 virtual private network. *Id.*

Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users transmitting data that is 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.* at ¶ 28. Thus, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33. *Id.*

Third, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33, 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 at least the foregoing reasons, Aventail fails to describe or suggest sending an access request message to the secure computer network address using a virtual private network communication link, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of independent claims 1, 17, and 33, along with their dependent claims 10, 12, 14, 26, 28, 30 and 31.

2. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 103(a) in view of Microsoft Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview") and RFC 1035

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent stand rejected under 35 U.S.C. § 103(a) as being unpatentable over VPN Overview in view of RFC 1035. The rejection is based on the reasons given on pages 19-25 and Appendix B of the Request. The Patent Owner respectfully traverses this rejection because (i) VPN Overview has not been shown to be prior

art, and (ii) assuming, *arguendo*, that VPN Overview qualifies as prior art, VPN Overview and RFC 1035, alone or in combination, have not been shown to teach, either expressly or inherently, each and every element of each of the independent claims 1, 17, and 33. The following remarks address each of these points in turn.

a) VPN Overview has not been show to qualify as prior art.

Both the Office Action and the Request assert that VPN Overview was published in 1998 without any stated support. Request at 5; Office Action at 2. The Patent Owner can only presume that these assertions arise from the copyright year printed on the face of the reference. *See*, VPN Overview at 2. As stated in Section I.B.3., above, this copyright date range is not the publication date of VPN Overview and the Office Action has failed to make any showing that it is. Indeed, the document is on its face identified as nothing more than a draft. VPN Overview at 1 (Stating the following: “White Paper – DRAFT”).

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that VPN Overview is prior art and requests all rejections based on VPN Overview be withdrawn. Nonetheless, the Patent Owner addresses VPN Overview below as though it is qualified prior art.

b) VPN Overview and RFC 1035 fail to teach, either expressly or inherently, each and every element of independent claims 1, 17, and 33 and fail to render those claims obvious.

VPN Overview and RFC 1035, either alone or in the proposed combination, fail to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33.

Here, VPN Overview provides an overview of VPNs, describing their basic requirements, and some of key technologies that permit private networking over public networks. *See*, VPN Overview at Abstract; Nieh Dec. at ¶ 30. For example, referring to FIG. 2 of VPN Overview, shown below, a VPN is shown to connect a remote user to a corporate Intranet. VPN Overview at 7; Nieh Dec. at ¶ 30. VPN Overview at 7. To this end, a user calls a local ISP and using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet. *See* VPN Overview at 8; Nieh Dec. at ¶ 30.

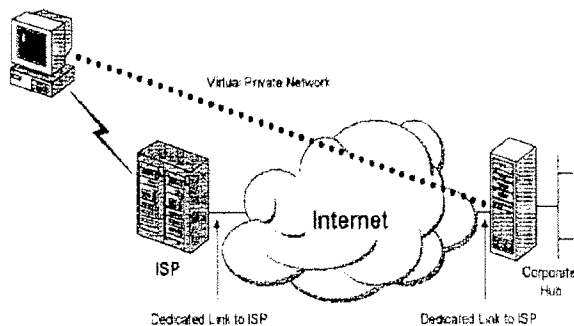


Figure 2: Using a VPN to connect a remote client to a private LAN

The Request asserts that a VPN tunnel server of the VPN Overview system can be identified using a domain name. Request at 21 (citing VPN Overview at page 26 asserting that the VPN tunnel server can be named “vpn.support.bigcompany.com”). The Request concludes and alleges that this domain name corresponds to a secure domain name because the domain name corresponds to a network address that requires authorization. *See* Request at 21. The Patent Owner respectfully disagrees for several reasons.

VPN Overview provides no indication that the client is sending a domain name to the Front End Processor (“FEP”) to establish a connection; instead, the indication is that the client is establishing a dial-up connection to the FEP. VPN Overview at 22 (stating “[i]n the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP.”); Nieh Dec. at ¶ 31. Even assuming for the sake of argument that the alleged domain name is sent from the client to the FEP, the VPN Overview provides no evidence that the alleged domain name is a secure domain name in the context of this application. Nieh Dec. at ¶ 31. A secure domain name, as recited in claim 1, 17, and 33 of the ‘180 Patent, is not a domain name that just happens to be associated with a computer used to establish a secure connection, as identified above at the outset of Section I.C. The Request alleges that VPN Overview describes a secure domain name because the domain name for the VPN tunnel server happens to correspond to a network address allegedly requiring authentication. *Id.* at ¶ 31. As stated at the outset of Section I.C., above, however, a secure domain name is not a domain name that so happens to correspond to a network address for a server involved in securing communications. *Id.*

The domain name of the VPN tunnel server is also not a secure domain name, even if this recitation is incorrectly defined according to the Request. *Id.* at ¶ 32. The Request asserts that a secure domain name corresponds to a secure computer network address. *Id.* However, the

address of the VPN tunnel server is not a secure computer network address, as stated above at the beginning of Section I.C. *Id.* Assuming for the sake of argument that a secure computer network address is associated with a computer which requires authorization for access, then, without authorization for access, a client computer cannot communicate with a secure computer network address. *Id.* In VPN Overview, however, a client computer may communicate with a VPN tunnel server without pre-authorization to access the hosts protected by the VPN tunnel server. *Id.* Thus, because the VPN tunnel server of the reference does not require authorization for access, it is not associated with a secure computer network address, and therefore also cannot be associated with a secure domain name. *Id.*

VPN Overview also has not been shown to teach or suggest a secure domain name service, as recited in claims 1, 17, and 33. VPN Overview, on page 26, describes that redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. *Id.* at ¶ 33. The round-robin DNS, however, is no different from a conventional DNS. *Id.* As stated above at the outset of Section I.C., a secure domain name service is not a conventional DNS. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

The Request appears to recognize these shortcomings of VPN Overview and therefore relies on RFC 1035 to supplement that reference. RFC 1035 is equally deficient. The Patent Owner respectfully submits that the proposed combination of VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name and a secure domain name service as recited in claims 1, 17, and 33. *Id.* at ¶ 34.

RFC 1035 describes user programs that interact with the domain name space through resolvers; the format of user queries and user responses is specific to the host and its operating system. RFC 1035 at 4; Nieh Dec. at ¶ 34. User queries will typically be operating system calls, and the resolver and its cache will be part of the host operating system. RFC 1035 at 4; Nieh Dec. at ¶ 34. Resolvers answer user queries with information they acquire via queries to foreign name servers and the local cache. RFC 1035 at 4; Nieh Dec. at ¶ 34.

Even assuming for the sake of the argument that this description supports the allegation that the user query corresponds to a domain name and the resolver corresponds to a domain name

Control Number: 95/001,270

service, RFC 1035 still fails to describe or suggest a secure domain name and a secure domain name service, as outlined at the outset of Section I.C., above. Nieh Dec. at ¶ 35. RFC 1035 is not seen to show anything other than a conventional DNS. *Id.* The Request also points to no evidence that distinguishes the alleged DNS of RFC 1035 from a conventional DNS. *Id.* at ¶ 36. Instead, the Request merely states that RFC 1035, on page 22, discloses that the domain name is sent to a domain name service for resolution and then passed back the IP address. Request at 22; *id.* As stated above in Section I.C., a secure domain name service unlike a conventional DNS. *Id.* Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.* As such, the proposed addition of subject matter from RFC 1035 fails to remedy the shortcomings of VPN Overview to describe or suggest a secure domain name or secure domain name service, as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 36.

Furthermore, the proposed combination of the VPN Overview and RFC 1035 also fails to describe or suggest a secure domain name or a secure domain name service even if these recitations are incorrectly defined as suggested by the Request. *Id.* at ¶ 37. The Request asserts that the secure domain name corresponds to a secure computer network address, and a secure domain name service corresponds to a lookup service that returns a secure network address for the requested secure domain name. Request at 21, 22. The proposed combination of the VPN Overview and RFC 1035 in fact does not teach these features. Nieh Dec. at ¶ 37.

The proposed combination of the VPN Overview and RFC 1035, at best, shows a DNS server that can allegedly receive the domain name of the VPN tunnel server and can allegedly resolve and return the IP address for the domain name of the VPN tunnel server. *Id.* at ¶ 38. As noted above, the issue is that the purpose of the VPN tunnel server is to secure a connection to resources behind the VPN tunnel server. *Id.* To this end, the VPN tunnel server itself is not secure – that is, it does not require authorization for access, as stated above at the outset of Section I.C. *Id.* Therefore, neither the domain name of the VPN tunnel server nor its corresponding computer network address is secure – even if this term is incorrectly defined as proposed by the Request. *Id.* As such, even under the Requester’s claim interpretation, the proposed combination of the VPN Overview and RFC 1035 fails to describe or suggest a secure domain name or a secure domain name service. *Id.*

As such, the proposed combination of the VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 39. For at least the foregoing reasons, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of independent claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

c) Secondary Considerations of Non-Obviousness

The Patent Owner presents in the §1.132 Declaration of Edmund Munger submitted herewith (“Munger Dec.”), objective evidence of non-obviousness of the rejected claims and a nexus between that evidence and the claimed inventions. This evidence is entitled to great weight as evidence of non-obviousness.

Perhaps most revealing is the jury verdict against the Requestor, Microsoft Corporation, finding that each of the independent claims here rejected, as well as some dependent claims, were not invalid and were willfully infringed by the Requester. Munger Dec. at ¶ 4. The jury awarded the Patent Owner **thirty four million dollars (\$34,000,000)** in damages stemming from infringement of the ‘180 Patent, including the independent claims rejected by the Office Action. *Id.* at ¶ 4. Because the rejected claims were found willfully infringed, the nexus is undeniable. The damage award is significant and clearly evinces significant commercial success.

Microsoft was not the only one seeing value in the claimed invention. SafeNet, a leading provider of Internet security technology that is the *de facto* standard in the VPN industry, entered into a portfolio license (which included the technology that became covered by the claims of the ‘180 Patent) in July 2002 to be incorporated into SafeNet’s VPNs. *Id.* at ¶ 12.

Considering the need for easy-to-use Internet security at the time of invention, the value of these inventions is not surprising. In 1998, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks. *Id.* at ¶ 10. In that time period, remote access was “a nightmare for support desks. Staffers never know what combination of CPU, modem, operating system and software configuration they’re going to have to support”, and adding the commercially available VPN software only made matters worse. *Id.* The computer and internet security industries were forced to chose between the ease of use and the security that the VPN system provided. *Id.* The inventions defined by claims 1, 17, and 33 of

the '180 Patent, combine both the ease of use and security aspects of a VPN, without sacrificing one or the other. *Id.*

In fact, prior to the invention of claims 1, 17 and 33 of the '180 Patent, there was significant and increasing concern with the security of computer communications. *Id.* at ¶ 5. In one example, the Defense Advanced Research Projects Agency (“DARPA”) provided significant funding for development of Internet security. DARPA provided funding of approximately \$130,000,000 from 1998 through 2000 alone. At least fifteen 15 different organizations were working on research, but none of them came up with the solution defined by claims 1, 17, and 33 of the '180 Patent. *Id.* at ¶ 7. In another example, In-Q-Tel, a company with strong ties to the U.S. CIA, funded the original development of secure remote connections technology to the tune of \$3,400,000. *Id.* at ¶ 8.

Recognizing the long felt need for these inventions, the original owner of the '180 Patent spent significant resources on their development. In fact, in the year the inventions were developed, it spent an amount in the development of these inventions nearly equal to its entire research and development budget for that year. *Id.* at ¶ 9.

The Examiner “must” consider secondary evidence of non-obviousness. MPEP 716.01(a). Such evidence is “often...the most probative and cogent evidence” of non-obviousness. *Demaco Corp. v. F. Von Langsdorff Licensing*, 851 F.2d 1387, 1391 (Fed. Cir. 1988). Secondary indicia of non-obviousness is entitled to “substantial weight” in the obviousness analysis when the Patent Owner establishes a nexus between the evidence and the claimed invention. *Stratoflex Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1539 (Fed. Cir. 1983).

For these additional reasons, the Patent Owner respectfully requests the withdrawal of the obviousness rejections of independent claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31 of the '180 Patent.

3. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(b) in view of Kosiur, “Building and Managing Virtual Private Networks” (hereafter “Kosiur”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent stand rejected under 35 U.S.C. § 102(b) as being anticipated by Kosiur. The rejection is based on the reasons given on pages 25-30 and Appendix C of the Request. The Patent Owner respectfully traverses this

rejection because Kosiur has not been shown to either expressly or inherently teach each and every element of each of the independent claims 1, 17, and 33.

Kosiur has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in each of claims 1, 17, and 33. Nieh Dec. at ¶ 40. Kosiur describes protecting external access to a company's intranet by establishing two corporate DNS servers: one external to the firewall and one internal. Kosiur at 295, 296; *Id.* The external corporate DNS includes a list of hosts that the company permits the public to access, such as, for example, the company's e-mail gateway, public web site, and anonymous FTP server. Kosiur at 296; Nieh Dec. at ¶ 40. The internal corporate DNS includes a list of hosts that only the company's internal network users are permitted to access. Kosiur at 296; Nieh Dec. at ¶ 40. When an internal host attempts to access an external host, the internal DNS server forwards the DNS request to the external DNS server. Kosiur at 296; Nieh Dec. at ¶ 40. In the reverse, however, if an external host attempts to access an internal host, then the external host must connect to the internal DNS server through a VPN. Kosiur at 296; Nieh Dec. at ¶ 40.

Although Kosiur describes a domain name, it does not describe a secure domain name, as recited in claims 1, 17, and 33. The Request asserts that Kosiur discloses domain name usage with VPN enabled servers and computers. *See* Request at 27. These domain names, the Request asserts, are "secure" because the domain names correspond to a network address that requires authentication. *See id.* This is incorrect. Nieh Dec. at ¶ 41. The Patent Owner respectfully submits that such a reading of a claim is contrary to its meaning and reads out a critical aspect of the invention. As identified at the outset of Section I.C., above, a secure domain name is not a domain name that just happens to correspond to a network address that requires authentication. Nieh Dec. at ¶ 41.

Kosiur has also not been shown to disclose a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 42. The Request alleges that a secure domain name service is a look-up request to a domain name service to resolve a domain name identifying VPN resources. Request at 27; Nieh Dec. at ¶ 42. Kosiur describes an internal DNS and an external DNS for resolving addresses of internal hosts and external hosts respectively. Request at 27; Nieh Dec. at ¶ 42. Kosiur has not been shown to disclose that either the internal or external DNS is different from a conventional DNS. Nieh Dec. at ¶ 42. Further, the Request provides no evidence that the DNS disclosed by Kosiur is different from conventional DNS. *Id.* The Request simply states

that “Kosiur discloses at pages 293-296 that domain name resolution occurs at DNS servers. The DNS servers pass back the corresponding network address.” Request at 28; Nieh Dec. at ¶ 42. Thus, Kosiur has not been shown to disclose anything other than a conventional DNS, and, as stated in Section I.C., above, a secure domain name service is not a conventional domain name service. Nieh Dec. at ¶ 42. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. Nieh Dec. at ¶ 42.

As such, Kosiur has not been shown to teach a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 43. For at least the foregoing reasons, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

4. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(a) in view of Kaufman, “Implementing IPsec” (hereafter “Kaufman”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Kaufman. The rejection is based on the reasons given on pages 30-35 and Appendix D of the Request. The Patent Owner respectfully traverses this rejection because Kaufman has not been shown to either expressly or inherently teach each and every element of each of the independent claims 1, 17, and 33.

Kaufman has not been shown to teach a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. Kaufman discloses the use of IPsec to secure communications through the Internet using authentication and encryption. Kaufman at 2; Nieh Dec. at ¶ 44. Kaufman also describes a domain name service being an integral part of the Internet and of any normal IP network. Kaufman at 128; Nieh Dec. at ¶ 44. The domain name service is described as a protocol used to support hierarchical resolution of host names to IP addresses (and vice versa) in the Internet. Kaufman at 243; Nieh Dec. at ¶ 44. Kaufman also describes that a layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Kaufman at 142; Nieh Dec. at ¶ 44. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network. Kaufman at 142; Nieh Dec. at ¶ 44.

Based on the foregoing, the Request alleges that an IPsec connection request over the Internet for a secured resource can use, for example, a DNS server to resolve the request. Request at 31; Nieh Dec. at ¶ 44. Even assuming, *arguendo*, this assertion is correct, it falls short of describing a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 44.

Kaufman has not been shown to teach or disclose a secure domain name, as recited in claims 1, 17, and 33. *Id.* at ¶ 45. Similar to previous assertions, the Request suggests that Kaufman describes a secure domain name simply because it describes a domain name corresponding to a network address involving security (*e.g.*, a computer protected by a home network). *Id.* As stated at the outset of Section I.C., above, however, a secure domain name cannot be properly read to be a domain name that just happens to be associated with a computer network address requiring authentication because this interpretation is inconsistent with the meaning adopted by the inventors of the '180 Patent. *Id.*

Second, Kaufman also has not been shown to describe or suggest a secure domain name service, as recited in claims 1, 17, and 33. The Request alleges that a “secure domain name service” includes any lookup service that resolves a secure domain name.” Request at 32; Nieh Dec. at ¶ 46. Assuming, *arguendo*, that Kaufman discloses a secure domain name, Kaufman has not been shown to disclose a secure domain name service because it has only been shown to disclose a conventional DNS. Nieh Dec. at ¶ 46. As stated at the outset of Section I.C., above, however, a secure domain name service is not a conventional DNS. *Id.* Specifically, a secure domain name service is unlike a conventional DNS that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

Moving forward, the Request also seems to allege that Kaufman’s disclosure of DNS Security (“DNSSEC”) is a secure domain name service. Request at 33; Nieh Dec. at ¶ 47. To the extent Kaufman even discloses DNSSEC, that protocol merely teaches protecting the integrity of the traditional DNS resolution process. Nieh Dec. at ¶ 47. This “conventional scheme” of protecting the integrity of DNS resolution is also explicitly disclosed in column 40, lines 6-14 of the specification of the '180 Patent as being conventional:

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).

As noted above, the inventors had explicitly contemplated this “conventional scheme” of performing DNS resolution, and nevertheless claimed a secure domain name service as being something different. Nieh Dec. at ¶ 47. The addition of security to protect the integrity of a traditional DNS look-up, does not teach a secure domain name service for the same reasons as identified at the outset of Section I.C. *Id.* at ¶ 47.

As such, Kaufman has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 48. For at least the foregoing reasons, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of claims 1, 17, and 33 and dependent claims 10, 12-15, 26, and 28-31.

5. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 103(a) In View of Kaufman and James M. Galvin, “Public Key Distribution with Secure DNS” (hereafter “Galvin”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 103(a) as being obvious over Kaufman in view of Galvin. The rejection is based on the reasons given on pages 36-41 and Appendix E of the Request.

a) Kaufman and Galvin fail to teach, either expressly or inherently, each and every element of independent claims 1, 17, and 33 and fail to render those claims obvious.

The Patent Owner respectfully submits that neither Kaufman nor Galvin, individually or in combination, describe or suggest each and every element of each of the independent claims 1, 17, and 33. Kaufman’s teachings and deficiencies are identified immediately above in Section I.C.4. Galvin is cited to teach “a second type of ‘secure domain name service’ that includes digitally signed resource records.” Request at 38. Galvin discloses using a public key in the DNS resolution process to protect the integrity of the process. Galvin at §§ 1 and 3.2; Nieh Dec. at ¶ 50. This “conventional scheme” protecting the integrity of DNS resolution is also explicitly disclosed in the specification of the ‘180 Patent:

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).

Col. 40, ll. 6-14; Nieh Dec. at ¶ 50. Thus, the inventors had explicitly contemplated this “conventional scheme” of performing DNS resolution, and nevertheless claimed a secure domain name service as something different. *Id.*

Therefore, this aspect of Galvin does not teach the “secure domain name service” recited in claims 1, 17, and 33. Nieh Dec. at ¶ 51. The Request assumes that a “secure domain name service” is a conventional domain name service which issues a public key to ensure that the service is trustworthy. Request at 36; Nieh Dec. at ¶ 51. As stated above at the outset of Section I.C., disclosure of a conventional domain name service does not disclose a secure domain name service. *Id.* The addition of a public key to ensure the integrity of a DNS look-up does not teach a secure domain name service. *Id.* Accordingly, Galvin fails to remedy the shortcomings of Kaufman to describe or suggest a secure domain name service as recited in claims 1, 17, and 33. *Id.* Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

b) Secondary Considerations of Non-Obviousness

For the reasons stated in Section I.C.2.c above, it would not have been obvious to combine Kaufman and Galvin in the manner proposed in the Office Action. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

6. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(a) in View of Gauntlet® Firewall for Windows NT Administrator’s Guide Version 5.0 (hereafter “Gauntlet”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Gauntlet. The rejection is based on the reasons given on

pages 40-45 and Appendix F of the Request. The Patent Owner respectfully traverses this rejection because (i) Gauntlet has not been shown to be prior art under § 102(a) and (ii) even if it is assumed for the sake of argument that Gauntlet qualifies as prior art, Gauntlet has not been shown to either expressly or inherently teach each and every element of each of the independent claims 1, 17, and 33. The following remarks address each of these points in turn.

a) Gauntlet has not been shown to be prior art under § 102(a).

Both the Office Action and the Request assert that Gauntlet was published between 1998 and 1999 without any stated support. Request at 6; Office Action at 3. The Patent Owner can only presume that this assertion arises from the copyright date range printed on the face of the reference. *See* Gauntlet at *ii*. As stated in Section I.B.3., above, this copyright date range is not the publication date of Gauntlet and the Office Action has failed to make any showing that it is.

The closeness of proximity of the alleged publication date of Gauntlet to the April 26, 2000 priority date of the ‘180 Patent makes the availability of the reference even more dubious. Suppose the relied upon sections of the Gauntlet reference were created on December 31, 1999, and the copyright date range was accordingly amended to read “1998-1999.” Under these circumstances, it is possible that the document, although created, was not disseminated until after the April 26, 2000, four months after creation. Under these circumstances, Gauntlet clearly would not be eligible to be relied upon as prior art to the ‘180 Patent.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Gauntlet is prior art and requests all rejections based on Gauntlet be withdrawn. Nonetheless, the Patent Owner addresses Gauntlet below as though it is qualified prior art.

b) Gauntlet has not been shown to either expressly or inherently, teach each and every element of independent claims 1, 17, and 33.

(1) Gauntlet has not been shown to teach “a secure domain name” and “a secure domain name service”.

Gauntlet has not been shown to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Gauntlet is an administrator’s guide describing the use and operation of firewall software. According to Gauntlet, “[a] firewall is a single point of defense that protects one side from the other. In networking situations, this

Control Number: 95/001,270

usually means protecting a company’s private network from other networks to which it is connected.” Gauntlet at 1-1; Nieh Dec. at ¶ 52. Gauntlet teaches a system that prohibits all network traffic through the firewall unless it is “expressly permitted.” Gauntlet at 1-1; Nieh Dec. at ¶ 52.

The disclosed firewall operates as follows. The firewall necessarily must see the network traffic communicating with the protected side of the wall, *i.e.*, the private network. Gauntlet at 1-6; Nieh Dec. at ¶ 53. After receiving a packet, the firewall checks the source and destination address of the packet against its user-defined rules, and then checks the type of request sought. Gauntlet at 1-8; Nieh Dec. at ¶ 53. If the requested service is supported and authorized, the appropriate program is called and the request is processed. Gauntlet at 1-8; Nieh Dec. at ¶ 53.

When determining if access should be permitted or denied, the firewall checks the IP address provided in the packet request against the user-provided rules. Gauntlet at 5-1; Nieh Dec. at ¶ 54. The rules can be defined by hostname or by IP address. Gauntlet at 5-1; Nieh Dec. at ¶ 54. Because the received packet identifies sources and destinations by IP addresses, if the rule is defined by hostname, additional steps are taken to convert an IP address identified in the packet to a hostname. Gauntlet at 5-2; Nieh Dec. at ¶ 54. In other words, “the proxy must use DNS to map the source or destination address (in the packet) into a host name” – the proxy performs a reverse DNS lookup. Gauntlet at 5-2; Nieh Dec. at ¶ 54.

The Gauntlet firewall also offers Point-to-Point Tunneling Protocol (“PPTP”) services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. Gauntlet at 18-1; Nieh Dec. at ¶ 55. To allow PPTP connections, however, the administrator of the firewall “must advertise the IP address of the PPTP server” and users “must connect directly to the server IP address.” Gauntlet at 18-1; Nieh Dec. at ¶ 55. To “advertise” an IP address, as used in Gauntlet, merely requires that the IP address be accessible to the public. Nieh Dec. at ¶ 55.

Gauntlet has not been shown to describe or suggest a secure domain name as recited in claims 1, 17, and 33. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a secure domain name. *See* Request at 42; Nieh Dec. at ¶ 56. For the reasons stated at the outset of Section I.C., a secure domain name cannot be properly read to be a domain name that just

happens to be associated with a server which is used to establish PPTP connections between a client and a target. Nieh Dec. at ¶ 56.

Similarly, to the extent that Gauntlet describes a conventional DNS, a secure domain name service cannot be properly read to be a conventional DNS. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a secure domain name, and the resolution of that domain name into a network address occurs at a secure domain name service. Request at 42; Nieh Dec. at ¶ 57. First, Gauntlet discloses the administrator of the firewall “must advertise the IP address of the PPTP server” and users “must connect directly to the server IP address.” Gauntlet at 18-1; Nieh Dec. at ¶ 57. Gauntlet has not been shown to disclose a DNS resolution for a hostname for a PPTP server. Nieh Dec. at ¶ 57. Second, to the extent that Gauntlet describes a DNS, it describes a conventional DNS and not a secure DNS. Nieh Dec. at ¶ 57. As noted at the outset of Section I.C., a secure domain name service differs from a conventional DNS. Nieh Dec. at ¶ 57.

For at least these reason, Gauntlet fails to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33 and dependent claims 10, 12-15, 26, and 28-31.

(2) Gauntlet fails to teach “receiving from the secure domain name service a response message containing the secure computer network address.”

The Request alleges that the use of a PPTP service, offered by the Gauntlet firewall software, requires the use of a PPTP server whose network address is a secure computer network address. Nieh Dec. at ¶ 58. The Gauntlet firewall offers PPTP services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. Nieh Dec. at ¶ 58; Gauntlet at 18-1.

As outlined at the outset of Section I.C., the network address of a PPTP server is not a secure computer network address because it does not require authorization for access. Nieh Dec. at ¶¶ 11, 58. That is, a client can communicate with the PPTP server without authorization. *Id.*

For at least these reasons, Gauntlet fails to teach a secure computer network address, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests

reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

7. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 103(a) in View of “Microsoft Windows NT Technical Support Hands-on, Self-Paced Training for Supporting Version 4.0” (hereafter “Hands-On”) in view of “Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers” (hereafter “Installing NT”).

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hands-On in view of Installing NT. The rejection is based on the reasons given on pages 45-52 and Appendix G of the Request. The Patent Owner respectfully traverses this rejection because (i) Installing NT has not been shown to be prior art under § 103(a) and (ii) even if, for the sake of argument, Installing NT qualifies as prior art, Installing NT and Hands-On, alone or in combination, are not seen to show either expressly or inherently, each and every element of each of the independent claims 1, 17, and 33.

a) Installing NT has not been shown to be prior art.

Both the Office Action and the Request assert that Installing NT was published in 1997 without any stated support. Request at 6; Office Action at 3. The Patent Owner can only presume that this assertion arises from the copyright date range printed on the face of the reference. *See* Installing NT at *iii*. As stated in Section I.B.3., above, this copyright date range is not the publication date of Installing NT and the Office Action has failed to make any showing that it is. Further, the document, on its face, designates itself as a “White Paper.” Installing NT at cover page.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Installing NT is prior art and requests all rejections based on Installing NT be withdrawn. Nonetheless, the Patent Owner addresses Installing NT below as though it is qualified prior art.

b) Hands-On and Installing NT do not either expressly or inherently, teach each and every element of independent claims 1, 17, and 33.

- (1) Hands-On and Installing NT fail to teach a “secure domain name” or a “secure domain name service.”

Installing NT is a white paper on the PPTP network protocol. See Installing NT at 1; Nieh Dec. at ¶ 59. Installing NT discloses the creation of a phonebook entry to dial a PPTP server. Installing NT at 20-22; Nieh Dec. at ¶ 59. The Request refers to Figure 12 in Installing NT to disclose a domain name for a PPTP server; Figure 12 is reproduced below. Nieh Dec. at ¶ 59. The Request, at page 47, refers to this figure to state that “PPTP connections can be identified using domain names” by indicating that the “Entry name” in the Figure is the domain name. *Id.* This is incorrect. *Id.* The “Entry name” is simply an arbitrary name to identify the Phonebook entry. *Id.* It does not *correspond* to a domain name of a PPTP server that would be resolved via a “traditional DNS server” to the network address of the PPTP server, as asserted on page 48 of the Request. *Id.*

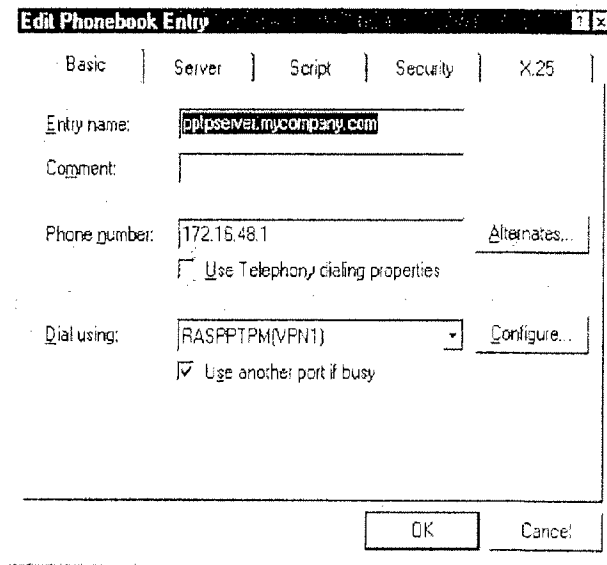


Figure 12 - Example Phonebook entry for PPTP server and a VPN device

Hands-On is a technical and training manual for Microsoft Windows NT. The Request describes Hands-On as disclosing PPTP, traditional DNS according to RFC 1035, and an AutoDial feature, which is described below. Request at 45-51; Nieh Dec. at ¶ 60.

Hands-On and Installing NT, either alone or in the proposed combination, fail to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. The Request alleges that Installing NT teaches that a name for a PPTP server is a

“secure domain name.” Nieh Dec. at ¶ 61; Request at 47. The Request asserts that, a PPTP server’s network address is a secure network address and that identifying the PPTP server with a domain name teaches a “secure domain name.” Nieh Dec. at ¶ 61. To the contrary, such an arbitrary identification is not a secure domain name. Nieh Dec. at ¶ 61. For the reasons stated above at the outset of Section I.C., a secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and a target. Nieh Dec. at ¶ 61. Neither the Office Action nor the Request demonstrate any aspect of Installing NT teaching anything other than a domain name that just happens to be associated with a PPTP server. Nieh Dec. at ¶ 61.

Hands-On similarly has not been shown to describe this feature. Nieh Dec. at ¶ 62. Notably, the Request does not rely on this reference to show this feature. As such, the Patent Owner does not believe that the proposed addition of subject matter from this reference remedies the shortcomings of Installing NT to describe or suggest a secure domain name. Nevertheless, for the reasons stated in Section I.C., to the extent that Hands-On discloses domain names, such a disclosure does not teach a secure domain name as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 62.

The Request also alleges that Hands-On discloses a secure domain name service. Request at 48-49; Nieh Dec. at ¶ 63. The Request asserts that Hands-On discloses two “lookup services” that allegedly disclose the secure domain name service recited in claim 1, 17, and 33. Request at 48; Nieh Dec. at ¶ 63. The first one is a “traditional DNS server.” Request at 48; Nieh Dec. at ¶ 63. According to the Request, sending a query message to a traditional DNS to resolve the domain name of the PPTP server disclosed in Installing NT (and described above) renders the traditional DNS a secure domain name service. Request at 48; Nieh Dec. at ¶ 63. For the reasons stated at the outset of Section I.C., a conventional DNS system is not transformed into a secure domain name service by merely resolving a query, that, unbeknownst to the secure domain name service, is requesting the address of a PPTP server.

The second “look-up service” disclosed in Hands-On also does not disclose the secure domain name service of claims 1, 17, and 33. Request at 48; Nieh Dec. at ¶ 64. This “alternative ‘lookup service’” is called AutoDial. Nieh Dec. at ¶ 64; Request at 48. AutoDial “maps and maintains network addresses to phonebook entries” such that, when an application or command requests access to an IP address, the client computer will match that network address

to the phonebook entry and dial the phone number associated with that network address. Hands-On at 462; Nieh Dec. at ¶ 64. Although an AutoDial database can include IP addresses and Internet host names, these addresses are each associated with a phonebook entry, which provides a phone number to be dialed for connecting with said IP addresses and Internet host names. Nieh Dec. at ¶ 64. Thus, AutoDial is not disclosed to resolve domain names to IP addresses, much less to resolve a secure domain name into a secure computer network address. Nieh Dec. at ¶ 64. Nevertheless, even assuming for the sake of argument that AutoDial were shown to teach a conventional DNS, a conventional DNS does not teach a secure domain name service for the reasons stated above at the outset of Section I.C. Nieh Dec. at ¶ 64.

As such, this alternative implementation also fails to describe or suggest a secure domain name service as recited in claim 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of independent claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

(2) Hands-On and Installing NT fail to describe or suggest receiving from a secure domain name service a secure computer network address

The Request alleges that, because a PPTP server, which enables a PPTP connection between a client and a target, may be referenced by a domain name, its domain name is a “secure domain name” and its network address is a “secure computer network address.” Request at 47; Nieh Dec. at ¶ 65. The network address for a PPTP server is not a secure network address because a client can communicate with it without authorization, as stated above at the outset of Section I.C. Nieh Dec. at ¶¶ 65, 11.

As such, the cited documents have not been shown to describe or suggest “receiving from a secure domain name service a secure computer network address,” as recited in claims 1, 17, and 33. Accordingly, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

c) Secondary Considerations of Non-Obviousness

For the reasons stated in Section I.C.2.c above, it would not have been obvious to combine Hands-On and Installing NT in the manner proposed in the Office Action. Therefore,

the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

8. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(a) in View of “Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources” (hereafter “Microsoft VPN”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Microsoft VPN. The rejection is based on the reasons given on pages 52-56 and Appendix H of the Request. The Patent Owner respectfully traverses this rejection because (i) Microsoft VPN has not been shown to be prior art under § 102(a) and (ii) even if, for the sake of argument, Microsoft VPN qualifies as prior art, Microsoft VPN has not been shown to either expressly or inherently, teach each and every element of each independent claim 1, 17, and 33.

a) Microsoft VPN has not been shown to be prior art under §102(a).

Both the Office Action and the Request assert that Microsoft VPN was published in on January 1, 2000, without any stated support. Request at 6; Office Action at 3. The Patent Owner can only presume that this assertion arises from the date printed on the face of the reference. *See* Microsoft VPN at cover page. As stated in Section I.B.3., above, this copyright date range is not the publication date of Microsoft VPN and the Office Action has failed to make any showing that it is.

Further, the closeness of proximity of the alleged publication date of Microsoft VPN to the April 26, 2000 priority date of the ‘180 Patent makes the availability of this reference as prior art even more dubious. Suppose the relied upon sections of the Microsoft VPN were actually created on “January 1, 2000.” Under these circumstances, it is possible that the document, although created, was not disseminated until after the priority date of the ‘180 Patent, four months after creation. Under these circumstances, Microsoft VPN clearly would not be eligible to be relied upon as prior art to the ‘180 Patent.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Microsoft VPN is prior art and requests all rejections based on Microsoft VPN be

withdrawn. Nonetheless, the Patent Owner addresses Microsoft VPN below as though it is qualified prior art.

b) Microsoft VPN has not been shown to either expressly or inherently, teach each and every element of independent claims 1, 17, and 33.

(1) Microsoft VPN fails to teach a “secure domain name” or “secure domain name service.”

Microsoft VPN is a compilation of various Microsoft documents. As identified by the Request, Microsoft VPN discloses PPTP connections for remote users to access a corporate network. Request at 52; Nieh Dec. at ¶ 66. Microsoft VPN discloses creating an IP address or host name of a corporate office “VPN” server. Microsoft VPN at 32; Nieh Dec. at ¶ 66. Microsoft VPN also discloses a conventional DNS structure. Microsoft VPN at 64-66; Nieh Dec. at ¶ 66. Microsoft VPN, however, has not been shown to teach a secure domain name or secure domain name service, as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 66.

The Request asserts that the hostname associated with a PPTP server, which is used to establish PPTP connections between a client and a target computer is a “secure domain name.” Request at 54; Nieh Dec. at ¶ 67. A secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and target for the reasons stated at the outset of Section I.C., above. Nieh Dec. at ¶ 67.

The Request also alleges that, since Microsoft VPN discloses a conventional DNS, which resolves domain names, a DNS request for the IP address for a PPTP server renders the traditional DNS a secure domain name service. Request at 54; Nieh Dec. at ¶ 68. This is incorrect. A conventional DNS is not transformed into a secure domain name service merely by resolving a request for the IP address of a server which is used to establish PPTP connections. Nieh Dec. at ¶ 68. As stated at the outset of Section I.C., above, disclosure of a conventional DNS does not disclose a secure domain name service. Nieh Dec. at ¶ 68. Accordingly, because Microsoft VPN does not describe or suggest a secure domain name or a secure domain name service as recited in claims 1, 17, and 33, the Patent Owner respectfully requests that reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26 and 28-31.

- (2) Microsoft VPN fails to teach receiving from a secure domain name service a computer network address.

The Request alleges that the network address of a PPTP server, which enables a PPTP connection between a client and a target, is a “secure computer network address.” Request at 54; Nieh Dec. at ¶ 69. The network address for a PPTP server is not a secure network address because a client can communicate with it without authorization, as stated above at the outset of Section I.C. Nieh Dec. at ¶¶ 69, 11.

Accordingly, because Microsoft VPN does not teach “a secure computer network address,” the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of claims 1, 17, and 33 and dependent claims 10, 12-15, 26, and 28-31.

II. Conclusion

For at least the reasons set forth above, the rejection of claims 1, 10, 12-15, 17, 26, 28-31, and 33 should be withdrawn. Reconsideration and prompt confirmation of claims 1, 10, 12-15, 17, 26, 28-31, and 33 are respectfully requested.

Please charge our Deposit Account No. 501133 any fees or credit any overcharges relating to this Response.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Patent Owner

28 State Street
Boston, MA 02109-1775
Phone: 617.535.4000
Facsimile: 617.535.3800
Date: April 19, 2010

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
 Edmund Munger, et al.)
)
 U.S. Patent No.: 7,188,180)
 Filed: November 7, 2003) Examiner:
 Issued: March 6, 2007) Andrew L. Nalven
)
 For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
 SECURE COMMUNICATION LINK)
 BETWEEN COMPUTERS OF)
 VIRTUAL PRIVATE NETWORK)
)
 Reexamination Proceeding)
 Control No.: 95/001,270)
 Filed: December 8, 2009)

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Response to Office Action in Reexamination, filed with United States Patent and Trademark Office on April 19, 2010, was served this 19th day of April, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
 Rothwell, Figg, Ernst & Manbeck, P.C.
 1425 K Street N.W.
 Suite 800
 Washington, D.C. 20005

Respectfully submitted,
 McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
 Toby H. Kusmer, P.C., Reg. No. 26,418
 Matthew E. Leno, Reg. No. 41,149
 Hasan M. Rashid, Reg. No. 62,390
 McDermott Will & Emery LLP
 Attorneys for Patent Owner
**Please recognize our Customer No. 23630 as
 our correspondence address.**

28 State Street
 Boston, MA 02109-1775
 Telephone: (617) 535-4000
 Facsimile: (617)535-3800
 tkusmer@mwe.com,
 mleno@mwe.com
 hrashid@mwe.com
Date: April 19, 2010

BST99 1648165-1.077580.0090

Electronic Acknowledgement Receipt

EFS ID:	7444576
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	077580-0090
Receipt Date:	19-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:25:13
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response after non-final action-owner timely	Response.pdf	1902408 <small>081bf379f4462cb5dae3ddf6251c64a5da22fd0a</small>	no	34

Warnings:

Information:

2	Reexam Certificate of Service	Cert_Serv_Resp.pdf	23959 6087a0aa8d2f73291d9a55ab0020c1622b766e8e	no	1
---	-------------------------------	--------------------	---------------------------------------------------	----	---

Warnings:

Information:

Total Files Size (in bytes):	1926367
-------------------------------------	---------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Patent Application Fee Transmittal

Application Number:	95001270
Filing Date:	08-Dec-2009
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	077580-0090

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Petition fee- 37 CFR 1.17(f) (Group I)	1462	1	400	400

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				400

Electronic Acknowledgement Receipt

EFS ID:	7444642
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	19-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:35:27
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$400
RAM confirmation Number	6258
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	Petition for review/processing depending on status	OPLA_Petition_pdf.pdf	28119 1380bbb6dd3350b3b887f591278e3ed47474c4c9	no	2

Warnings:

Information:

2	Reexam Certificate of Service	Cert_Serv_OPLA_Petition.pdf	27525 109eb2ca7d734b8445571a47bd1e4dea1bf0a76	no	1
---	-------------------------------	-----------------------------	--------------------------------------------------	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	30501 0609da24d685dd75e7f4897387b0f39404f24e15	no	2
---	-------------------------	--------------	---------------------------------------------------	----	---

Warnings:

Information:

Total Files Size (in bytes):

86145

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 the Reexamination of:)
 Edmund Munger, et al.)
)
 U.S. Patent No.: 7,188,180)
 Filed: November 7, 2003) Examiner:
 Issued: March 6, 2007) Andrew L. Nalven
)
 For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
 SECURE COMMUNICATION LINK)
 BETWEEN COMPUTERS OF)
 VIRTUAL PRIVATE NETWORK)
)
 Reexamination Proceeding)
 Control No.: 95/001,270)
 Filed: December 8, 2009)

Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132

Pursuant to 37 C.F.R. § 1.132, I declare that the following statements are true to the best of my knowledge, information, and belief, formed after reasonable inquiry under the circumstances.

Background

1. I have over 15 years of experience with operating systems and distributed systems. More specifically, my experience includes remote access, computer networking, and computer security. Examples of my experience are evidenced by my publication of papers in top-tier networking and security conferences, service on programming committees for networking and security conferences, awards for research work, and receipt of research grants in the field of networking and security. My qualifications, including a description of all of this information, may be found in my curriculum vitae, which is attached hereto as Exhibit A.

2. I earned a Bachelor of Science degree from the Massachusetts Institute of Technology in Electrical Engineering in 1989. I earned a Masters of Science degree from Stanford University in Electrical Engineering in 1990. I also received my Ph.D. in Electrical Engineering from Stanford University in 1999.

3. I joined Columbia University as a faculty member in 1999, where I am now a tenured Associate Professor in the Department of Computer Science. I am also currently the director of the Network Computer Laboratory at Columbia University.

4. My research interests include mobile computing, operating systems, distributed systems, thin-client computing, web and multimedia systems, and performance evaluation. I have

supervised a number of Ph.D. students who worked on and completed dissertations in the area of networking and security. I also teach courses in advanced operating systems and mobile computing, both of which involve computer networking and security.

5. I have also served as an expert in various litigations in the fields of computer networking and security, which include virtual private networking.

Resources I have Consulted

6. I have been retained by the Patent Owner, VirnetX, Inc., to offer my opinion of the patentability of claims 1, 10, 12-15, 17, 26, 28-31, and 33 of U.S. Patent No. 7,188,180 (“the ‘180 Patent”) in view of the Office Action dated January 19, 2010 (“the Office Action”) received by the Patent Owner in the reexamination of the ‘180 Patent.

7. In preparing this declaration, I have reviewed the ‘180 Patent. I have also reviewed the Office Action. I have also reviewed the Request for *Inter Partes* Reexamination of Patent (“the Request”) to the extent it is adopted by the Office Action. I have also reviewed Appendices A-H to the Request to the extent that they are adopted in the Office Action. Lastly, I have reviewed the references upon which the rejections in the Office Action are based, namely Aventail Connect v3.1/v2.6 Administrator’s Guide (“Aventail”); Microsoft Windows NT Server, Virtual Private Networking: An Overview (“VPN Overview”); IETF RFC 1035 (“RFC 1035”); Kosiur, “Building and Managing Virtual Private Networks” (“Kosiur”); Kaufman, “Implementing IPsec” (“Kaufman”); James M. Galvin, “Public Key Distribution with Secure DNS” (“Galvin”); “Gauntlet® Firewall for Windows NT Administrator’s Guide Version 5.0 (“Gauntlet”); “Microsoft Windows NT Technical Support Hands-on, Self-Paced Training for Supporting Version 4.0” (“Hands-On”); “Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers” (“Installing NT”); and “Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources” (“Microsoft VPN”).

8. A detailed explanation of the basis for my opinions is set forth in the remainder of this declaration.

Detailed Basis for My Opinion

Secure Domain Name and Secure Domain Name Service

9. As I stated above, I have read the ‘180 Patent and understand independent claims 1, 17, and 33 recite a secure domain name and a secure domain name service.

10. As I read the Office Action and the Request, those documents rely on the erroneous premise that a secure domain name is a domain name that just happens to correspond to a secure computer. Alternatively, the Request and Office Action rely on the faulty position that a secure domain name corresponds to an address that simply requires authorization. These assertions are in clear contradiction of the specification to the ‘180 Patent, which takes pains to explain that a secure domain name is different from a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization, as shown in the ‘180 Patent at column 51, lines 18-32. To illustrate, in various implementations,

the '180 Patent describes that a secure domain name is a "a non-standard domain name." Examples of such non-standard domain names are described in Claim 11: .scom, .snet, .sorg, .sedu, .smil, and .sgov. Dependent claim 2 also differentiates between a secure domain name and a non-secure domain name in reciting the step of "automatically generating a secure domain name corresponding to a non-secure domain name." To further illustrate, the '180 Patent describes, at column 51, lines 28-32, that "a query [with a secure domain name] to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." Thus, the inventors demonstrated that the secure domain name recited in claims 1, 17, and 33 of the '180 Patent cannot be properly read to be a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization. As seen from the previous sentences, a secure domain name is different from a domain name that just happens to be associated with a secure computer or secure computer network address. For example, as pointed above, the domain name that just happens to correspond to a secure computer or a domain name that just happens to correspond to an address requiring authentication can be resolved, for example, by a conventional domain name service; whereas, as noted above, a secure domain name cannot be resolved by a conventional domain name service, for example.

11. Furthermore, even if the recitation "secure domain name" is defined according to the Request to mean a domain name corresponding to a secure computer or a domain name corresponding to an address requiring authorization for access, various of the cited documents still fail to describe or suggest this feature. Specifically, the relied upon portions of the cited documents describe domain names of computers that do not require authorization for access. Instead, the computers (*e.g.*, a VPN tunnel server or a PPTP server) of the cited documents are for securing a connection between a client computer and a target computer. To this end, the computers (*e.g.*, a VPN tunnel server or a PPTP server) themselves do not have a secure computer network address because they do not require authorization for access or authorization for a client computer to communicate with them. Any client computer can, without authorization, communicate with one of these alleged computers (*e.g.* a VPN tunnel server or a PPTP server); it is the target computer that may require authorization for access. Therefore, neither the domain name of the alleged computers (*e.g.*, a VPN tunnel server or a PPTP server) nor their corresponding computer network address is secure – even if this term is defined according to the Request. As such, these cited documents do not teach a secure computer network address or, correspondingly, a secure domain name.

12. Similarly, the Request and Office Action rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of secure computers. Alternatively, the Request and Office Action also rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of computers that are used to establish a secure connection, such as a VPN tunnel server or a PPTP server. Again, these arguments are belied by the '180 Patent itself. The specification of the '180 Patent, including column 51, lines 29-45 and column 52, lines 4-26, clearly teaches that the claimed secure domain name service of claims 1, 17, and 33 is unlike a conventional domain name service, which the inventors understood as including both DNS and DNS with public key security according to column 40, lines 6-17 of the '180 Patent. To illustrate, the '180 Patent explicitly states 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: in an embodiment described at column 51, lines 18-45, the '180 Patent states that "[b]ecause 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." A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name. A secure domain name service of the '180 Patent, instead, recognizes that a query message is requesting a secure computer network address and performs its services accordingly. Furthermore, in various implementations, the '180 Patent describes a secure domain name service as providing additional functionalities not available with a conventional domain name service, as described above in the '180 Patent at column 52, lines 4-26. The '180 Patent, at column 40, lines 6-17, even describes the drawbacks of the conventional scheme of a traditional DNS and public key security:

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

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

Thus, it is my belief that the secure domain name service recited in claims 1, 17, and 33 of the '180 Patent is different from a conventional domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

13. Given my statements above, I do not believe that the references cited in the Office Action teach or disclose the secure domain name and secure domain name service recited in claims 1, 17, and 33.

The Aventail Reference

14. After reviewing the Aventail reference, I understand Aventail to disclose a system and architecture for transmitting data between two computers using the SOCKS protocol. The system according to Aventail routes certain, predefined network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, possibly through successive servers. Upon receipt of the network traffic, the SOCKS server is disclosed to transmit the network traffic to the Internet or external network. Aventail's disclosure is limited to connections created at the socket layer of the network architecture.

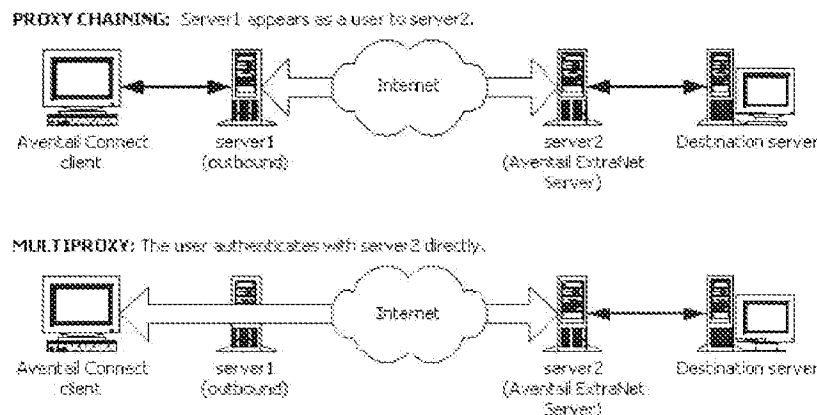
15. I note that pages 9-12 of Aventail discuss the basics of the operation of Aventail Connect, the software necessary to implement the system disclosed in Aventail. According to page 9 of Aventail, a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. Accordingly, the Aventail Connect

software is disclosed to intercept all connection requests from the user, and determines whether each request matches local, preset criteria for redirection to a SOCKS server.

16. According to page 12 of Aventail, if redirection is appropriate, then Aventail Connect creates a false DNS entry to return to the requesting application. Aventail discloses that Aventail Connect then forwards the destination hostname identified in the DNS request to the extranet SOCK server over a SOCKS connection.

17. Although Aventail is generally silent on the operation of the SOCKS server, I understand from page 12 that the SOCKS server performs the hostname resolution. Once the hostname is resolved, the user can transmit data over a SOCKS connection to the SOCKS server. The SOCKS server, then, separately relays that transmitted data to the target.

18. Page 12 of the Request, adopted by the Examiner in the Office Action, also cites the “Proxy Chaining” and “MultiProxy” modes disclosed in Aventail at pages 68-73. I have reproduced below a figure taken from page 72 of Aventail depicting these two modes.



19. In the “Proxy Chaining” mode, Aventail discloses that a user can communicate with a target via a number of proxies such that each proxy server acts as a client to the next downstream proxy server. As shown above, in this mode, the user does not communicate directly with the proxy servers other than the one immediately downstream from it.

20. In the “MultiProxy” mode, Aventail discloses that the user, via Aventail Connect, connects through each successive proxy server directly.

21. Regardless of whether one of these modes is enabled, as shown in the figure, an external SOCKS server is necessary and the operation of Aventail Connect, for the purposes of my opinion, does not materially differ based on whether one of these modes is enabled.

22. The Office Action at page 6 asserts that a hostname (*e.g.*, the alleged secure domain name) is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption. It thus interprets a secure domain name to be a domain name associated with a secure computer. This is incorrect for the reasons I stated in ¶¶ 9-12.

23. The Office Action at page 7 also suggests that a DNS server that can resolve addresses of secure computers corresponds to a secure domain name service. Aventail has not been shown

to teach anything more than a conventional DNS. As I stated in ¶¶ 9-12, however, a secure domain name service cannot be properly read to be a conventional domain name service. A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

24. The Request at page 15 also asserts that Aventail discloses two look-up services, alleged to be described on pages 8 and 12 of that reference. On page 8, Aventail discloses the traditional protocol for a computer to connect to a remote host. On page 12, Aventail discloses “forward[ing] the host-name to the extranet (SOCKS) server [where] the SOCKS server performs the hostname resolution.” Here, Aventail has not been shown to disclose anything other than a traditional DNS. As I stated in ¶¶ 9-12, however, a secure domain name service is unlike a conventional domain name service. A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. As such, Aventail fails to teach a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33.

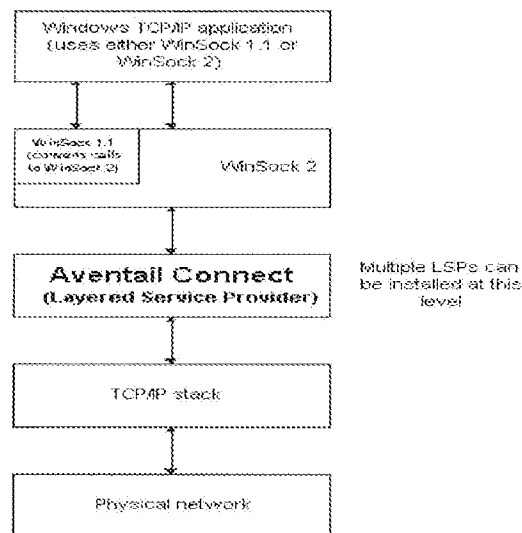
25. Aventail also has not been shown to teach sending an access request message to a secure computer network address using a virtual private network communication link, as recited in claims 1, 17, and 33. The links created by the systems and methods disclosed in Aventail differ from the virtual private network communication link recited in claims 1, 17, and 33. 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. Aventail discloses establishing point-to-point SOCKS connections between a client computer and a SOCKS server. The SOCKS server then relays data received to the intended target. Aventail does not disclose a virtual private network, as recited in claims 1, 17, and 33, where data can be addressed to one or more different computers across the network, regardless of the location of the computer.

26. For example, suppose two computers, A and B, reside on a public network. Further, suppose two computers, X and Y, reside on a private network. 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. This is true because A, B, X, and Y would all be a part of the same virtual private network.

27. 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. 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. This is one example of how the cited portions of Aventail fail to disclose a virtual private network.

28. Second, according to Aventail, Aventail Connect’s fundamental operation is incompatible with users transmitting data that is sensitive to network information. As stated

above, Aventail discloses that Aventail Connect operates between the WinSock and TCP/IP layers, as depicted on page 9:



Because Aventail discloses that Aventail Connect operates between these layers, it can intercept DNS requests. 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. Accordingly, Aventail discloses that the user will receive false network information from Aventail Connect for these hostnames. 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. Thus, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33.

29. Third, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33, because computers connected according to Aventail do not communicate directly with each other. 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. The SOCKS server then relays that data to a target computer on a private network on which the SOCKS server also resides. All communications between the client and target stop and start at the intermediate SOCKS server. 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. Instead, the client computer and target computer are deliberately separated by the intermediate SOCKS server.

The VPN Overview and RFC 1035 References

30. According to its abstract, VPN Overview provides an overview of VPNs, describing their basic requirements, and some of key technologies that permit private networking over public networks. For example, referring to FIG. 2 of VPN Overview, which I have reproduced below, a VPN is shown to connect a remote user to a corporate Intranet.

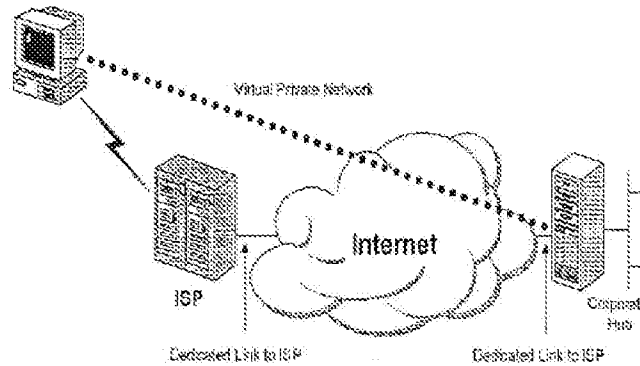


Figure 2: Using a VPN to connect a remote client to a private LAN

To this end, according to page 8 of VPN Overview, a user calls a local ISP and using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

31. VPN Overview provides no indication that the client is sending a domain name to the Front End Processor (“FEP”) to establish a connection; instead, the indication is that the client is establishing a dial-up connection to the FEP. At page 22, VPN Overview states “[i]n the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP.” Even assuming for the sake of argument that the alleged domain name is sent from the client to the FEP, the VPN Overview provides no evidence that the alleged domain name is a secure domain name in the context of this application. As I stated in ¶¶ 9-12, a secure domain name, as recited in claims 1, 17, and 33 of the ‘180 Patent, is not a domain name that just happens to be associated with a computer used to establish a secure connection. The Request also alleges that VPN Overview describes a secure domain name because the domain name for the VPN tunnel server happens to correspond to a network address allegedly requiring authentication. As I stated in ¶¶ 9-12, however, a secure domain name is not a domain name that so happens to correspond to a network address for a server involved in securing communications.

32. The domain name of the VPN tunnel server is also not a secure domain name, even if this recitation is incorrectly defined according to the Request. The Request asserts that a secure domain name corresponds to a secure computer network address. However, the address of the VPN tunnel server is not a secure computer network address, for the reasons I stated in ¶ 11. Assuming for the sake of argument that the Request correctly interprets a secure computer network address to be associated with a computer which requires authorization for access, then, without authorization for access, a client computer cannot communicate with a secure computer network address. In VPN Overview, however, a client computer may communicate with a VPN tunnel server without pre-authorization to access the hosts protected by the VPN tunnel server. Thus, because the VPN tunnel server of the reference does not require authorization for access, it is not associated with a secure computer network address, and therefore also cannot be associated with a secure domain name.

33. VPN Overview also has not been shown to teach a secure domain name service. VPN Overview, on page 26, describes that redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common

security perimeter. The round-robin DNS, however, is no different from a conventional DNS. As I stated in ¶¶ 9-12, however, a secure domain name service is not a conventional DNS. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

34. The proposed combination of VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name and a secure domain name service as recited in claims 1, 17, and 33. RFC 1035, at page 4, describes user programs that interact with the domain name space through resolvers; the format of user queries and user responses is specific to the host and its operating system. User queries will typically be operating system calls, and the resolver and its cache will be part of the host operating system. Resolvers answer user queries with information they acquire via queries to foreign name servers and the local cache.

35. Even assuming for the sake of the argument that this description supports the allegation that the user query corresponds to a domain name and the resolver corresponds to a domain name service, RFC 1035 still fails to describe or suggest a secure domain name and a secure domain name service, as I outlined in ¶¶ 9-12 above. RFC 1035 is not seen to show anything other than a conventional DNS.

36. The Request also points to no evidence that distinguishes the alleged DNS of RFC 1035 from a conventional DNS. Instead, the Request merely states that RFC 1035, on page 22, discloses that the domain name is sent to a domain name service for resolution and then passed back the IP address. As stated above in ¶¶ 9-12, a secure domain name service is unlike a conventional DNS. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. As such, the proposed addition of subject matter from RFC 1035 fails to remedy the shortcomings of VPN Overview to describe or suggest a secure domain name or secure domain name service, as recited in claims 1, 17, and 33.

37. Furthermore, the proposed combination of the VPN Overview and RFC 1035 also fails to describe or suggest a secure domain name or a secure domain name service even if these recitations are incorrectly defined as suggested by the Request. The Request, at pages 21-22, asserts that the secure domain name corresponds to a secure computer network address, and a secure domain name service corresponds to a lookup service that returns a secure network address for the requested secure domain name. The proposed combination of the VPN Overview and RFC 1035, in fact, does not teach these features.

38. The proposed combination of the VPN Overview and RFC 1035, at best, shows a DNS server that can allegedly receive the domain name of the VPN tunnel server and can allegedly resolve and return the IP address for the domain name of the VPN tunnel server. As noted above, the issue is that the purpose of the VPN tunnel server is to secure a connection to resources behind the VPN tunnel server. To this end, for the reasons I stated in ¶ 11, the VPN tunnel server itself is not secure – that is, it does not require authorization for access. Therefore, neither the domain name of the VPN tunnel server nor its corresponding computer network address is secure – even if this term is defined as proposed by the Request.

39. As such, even under the Request's incorrect claim interpretation, the proposed combination of the VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

The Kosiur Reference

40. Kosiur has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. At pages 295-96, Kosiur describes protecting external access to a company's intranet by establishing two corporate DNS servers: one external to the firewall and one internal. The external corporate DNS includes a list of hosts that the company permits the public to access, such as, for example, the company's e-mail gateway, public web site, and anonymous FTP server. The internal corporate DNS includes a list of hosts that only the company's internal network users are permitted to access. When an internal host attempts to access an external host, the internal DNS server forwards the DNS request to the external DNS server. In the reverse, however, if an external host attempts to access an internal host, then the external host must connect to the internal DNS server through a VPN.

41. Although Kosiur describes a domain name, it does not describe a secure domain name, as recited in claims 1, 17, and 33. The Request asserts that Kosiur discloses "domain name usage with VPN enabled servers and computers." These domain names, the Request asserts, are "secure" because the domain names correspond to a network address that requires authentication. This is incorrect. Such a reading of a claim is contrary to its meaning and reads out a critical aspect of the invention. For the reasons I stated in ¶¶ 9-12, a secure domain name is not a domain name that just happens to correspond to a network address that requires authentication.

42. Kosiur has also not been shown to disclose a secure domain name service, as recited in claims 1, 17, and 33. The Request alleges that a secure domain name service is a look-up request to a domain name service to resolve a domain name identifying VPN resources. Kosiur describes an internal DNS and an external DNS for resolving addresses of internal hosts and external hosts respectively. Kosiur has not been shown to disclose that either the internal or external DNS is different from a conventional DNS. Further, the Request provides no evidence that the DNS disclosed by Kosiur is different from a conventional DNS. The Request, at page 28 simply states that "Kosiur discloses at pages 293-296 that domain name resolution occurs at DNS servers. The DNS servers pass back the corresponding network address." Thus, Kosiur has not been shown to disclose anything other than a conventional DNS, and, as I stated in ¶¶ 9-12, a secure domain name service is not a conventional domain name service. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

43. As such, Kosiur has not been shown to teach a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

The Kaufman Reference

44. At page 2, Kaufman discloses the use of IPsec to secure communications through the Internet using authentication and encryption. At page 128, Kaufman also describes a domain name service being an integral part of the Internet and of any normal IP network. At page 243, the domain name service is described as a protocol used to support hierarchical resolution of host names to IP addresses (and vice versa) in the Internet. Kaufman also describes that a layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network. The Request alleges that an IPsec connection request over the Internet for a secured resource can use, for example, a DNS server to resolve the request. Even assuming, *arguendo*, this assertion is correct, it falls short of describing a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

45. Kaufman has not been shown to teach or disclose a secure domain name, as recited in claims 1, 17, and 33. Similar to previous assertions, the Request suggests that Kaufman describes a secure domain name simply because it describes a domain name corresponding to a network address involving security (*e.g.* a computer protected by a home network). As I stated in ¶¶ 9-12, however, a secure domain name cannot be properly read to be a domain name that just happens to be associated with a computer network address requiring authentication because this interpretation is inconsistent with the meaning adopted by the inventors of the '180 Patent.

46. Kaufman also has not been shown to describe or suggest a secure domain name service, as recited in claims 1, 17, and 33. The Request, at page 32, alleges that a “‘secure domain name service’ includes any lookup service that resolves a secure domain name.” Assuming, for the sake of argument, that Kaufman discloses a secure domain name, Kaufman has not been shown to disclose a secure domain name service because it has only been shown to disclose a conventional DNS. As I provided in ¶¶ 9-12, a secure domain name service is unlike a conventional DNS. Specifically, a secure domain name service is not a conventional DNS that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

47. The Request also seems to allege that Kaufman’s disclosure of DNS Security (“DNSSEC”) is a secure domain name service. To the extent Kaufman even discloses DNSSEC, that protocol merely teaches protecting the integrity of the traditional DNS resolution process. This “conventional scheme” of protecting the integrity of DNS resolution is also explicitly disclosed in column 40, lines 6-14 of the specification of the '180 Patent as being conventional:

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).

As I noted above, the inventors had explicitly contemplated this “conventional scheme” of performing DNS resolution, and nevertheless claimed a secure domain name service as being something different. The addition of security to protect the integrity of a traditional DNS look-up does not teach a secure domain name service for the same reasons as I identified in ¶¶ 9-12.

48. Kaufman has not been shown to describe or suggest a secure domain name or a secure domain name service as recited in claims 1, 17, and 33.

The Kaufman and Galvin References

49. I incorporate here my statements made immediately above in ¶¶ 42-46 regarding Kaufman.

50. According to page 38 of the Request, Galvin is cited to teach “a second type of ‘secure domain name service’ that includes digitally signed resource records.” Galvin at §§ 1 and 3.2 discloses using a public key in the DNS resolution process to protect the integrity of the process. This “conventional scheme” protecting the integrity of DNS resolution is also explicitly disclosed in column 40, lines 6-14 of the specification of the ‘180 Patent:

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).

Thus, the inventors had explicitly contemplated this “conventional scheme” of performing DNS resolution, and nevertheless claimed a secure domain name service as being something different.

51. This aspect of Galvin does not teach the secure domain name service recited in claims 1, 17, and 33. The Request assumes that a “secure domain name service” is a conventional domain name service which issues a public key to ensure that the service is trustworthy. As I stated above, however, in ¶¶ 9-12, disclosure of a conventional domain name service does not disclose a secure domain name service. The addition of a public key to ensure the integrity of a DNS look-up does not teach a secure domain name service. As such, Galvin fails to remedy the shortcomings of Kaufman to describe or suggest a secure domain name service as recited in claims 1, 17, and 33.

The Gauntlet Reference

52. According to Gauntlet at page 1-1, “[a] firewall is a single point of defense that protects one side from the other. In networking situations, this usually means protecting a company’s private network from other networks to which it is connected.” Gauntlet teaches a system that prohibits all network traffic through the firewall unless it is “expressly permitted.”

53. The disclosed firewall operates as follows, as described on pages 1-6 to 1-8. The firewall necessarily must see the network traffic communicating with the protected side of the wall, *i.e.*, the private network. After receiving a packet, the firewall checks the source and destination address of the packet against its user-defined rules, and then checks the type of request sought. If the requested service is supported and authorized, the appropriate program is called and the request is processed.

54. According to pages 5-1 to 5-2, when determining if access should be permitted or denied, the firewall checks the IP address provided in the packet request against the user-provided rules. The rules can be defined by hostname or by IP address. Because the received packet identifies sources and destinations by IP addresses, if the rule is defined by hostname, additional steps are taken to convert an IP address identified in the packet to a hostname. In other words, “the proxy must use DNS to map the source or destination address (in the packet) into a host name” – the proxy performs a reverse DNS lookup.

55. According to chapter 18 of Gauntlet, the Gauntlet firewall also offers Point-to-Point Tunneling Protocol (“PPTP”) services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. To allow PPTP connections, however, the administrator of the firewall “must advertise the IP address of the PPTP server” and users “must connect directly to the server IP address.” To “advertise” an IP address, as used in Gauntlet, merely requires that the IP address be accessible to the public.

56. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a secure domain name. As I stated in ¶¶ 9-12, a secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and a target.

57. Similarly, to the extent that Gauntlet describes a conventional DNS, a secure domain name service cannot be properly read to be a conventional DNS. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a secure domain name, and the resolution of that domain name into a network address occurs at a secure domain name service. First, Gauntlet discloses at 18-1 that the administrator of the firewall “must advertise the IP address of the PPTP server” and users “must connect directly to the server IP address.” Gauntlet has not been shown to disclose a DNS resolution for a hostname for a PPTP server. Second, to the extent that Gauntlet describes a DNS, it describes a conventional DNS and not a secure DNS. As noted at the outset of Section I.C., a secure domain name service differs from a conventional DNS, as I demonstrated in ¶¶ 9-12.

58. The Request also alleges that the use of a PPTP service, offered by the Gauntlet firewall software, requires the use of a PPTP server whose network address is a secure computer network address. The Gauntlet firewall offers PPTP services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. The network address of a PPTP server, however, is not a secure computer network address because it does not require authorization for access, as I stated above in ¶ 11. That is, a client can communicate with the PPTP server without authorization.

The Hands-On and Installing NT References

59. Installing NT is a white paper on the PPTP network protocol. According to pages 20-22, Installing NT discloses the creation of a phonebook entry to dial a PPTP server. The Request refers to Figure 12 in that reference to disclose a domain name for a PPTP server; the Figure is reproduced below:

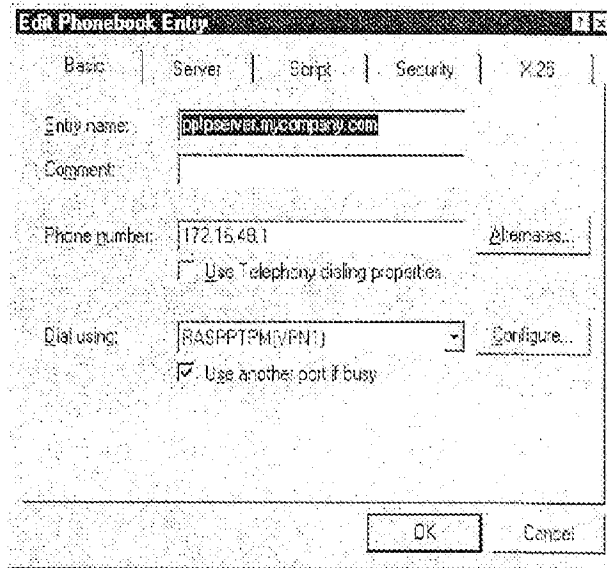


Figure 12 - Example Phonebook entry for PPTP server and a VPN device

The Request, at pages 47-48, refers to this figure to state that “PPTP connections can be identified using domain names” by indicating that the “Entry name” in the Figure is the domain name. This is incorrect. The “Entry name” is simply an arbitrary name to identify the Phonebook entry. It does not *correspond* to a domain name of a PPTP server that would be resolved to via a “traditional DNS server” to the network address of the PPTP server, as asserted on page 48 of the Request.

60. Hands-On is a technical and training manual for Microsoft Windows NT. The Request describes Hands-On as disclosing PPTP, traditional DNS according to RFC 1035, and an AutoDial feature, which I describe below.

61. The Request alleges that Installing NT teaches that a name for a PPTP server is a “secure domain name.” The Request, at page 47, asserts that a PPTP server’s network address is a secure network address and that identifying the PPTP server with a domain name teaches a “secure domain name.” To the contrary, such an arbitrary identification is not a secure domain name. As I demonstrated above in ¶¶ 9-12, a secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and a target. Neither the Office Action nor the Request demonstrate any aspect of Installing NT that teaches or discloses anything other than a domain name that just happens to be associated with a PPTP server.

62. Hands-On similarly has not been shown to describe this feature. Notably, the Request does not rely on this reference to show this feature. Nevertheless, for the reasons I stated in ¶¶ 9-

12, to the extent that Hands-On discloses domain names, such a disclosure does not teach or disclose a secure domain name, as recited in claims 1,17, and 33.

63. The Request also alleges that Hands-On discloses a secure domain name service. The Request asserts that Hands-On discloses two “lookup services” that allegedly disclose the secure domain name service recited in claims 1, 17, and 33. The first one is a “traditional DNS server.” According to the Request, sending a query message to a traditional DNS to resolve the domain name of the PPTP server disclosed in Installing NT (and described above) renders the traditional DNS a secure domain name service. As I stated previously at ¶¶ 9-12, a conventional DNS is not transformed into a secure domain name service by merely resolving a query, that, unbeknownst to the secure domain name service, is requesting the address of a PPTP server.

64. The second “look-up service” disclosed in Hands-On also does not disclose the secure domain name service of claims 1, 17, and 33. This “alternative ‘lookup service’” is called AutoDial. According to Hands-On at 462, AutoDial “maps and maintains network addresses to phonebook entries” such that, when an application or command requests access to an IP address, the client computer will match that network address to the phonebook entry and dial the phone number associated with that network address. Although an AutoDial database can include IP addresses and Internet host names, these addresses are each associated with a phonebook entry, which provides a phone number to be dialed for connecting with said IP addresses and Internet host names. Thus, AutoDial is not disclosed to resolve domain names to IP addresses, much less to resolve a secure domain name into a secure computer network address. Nevertheless, even assuming for the sake of argument that AutoDial were shown to teach a conventional DNS, a conventional DNS does not teach a secure domain name service, as I described in ¶¶ 9-12 above.

65. The Request also alleges that, because a PPTP server, which enables a PPTP connection between a client and a target, may be referenced by a domain name, its domain name is a “secure domain name” and its network address is a “secure computer network address.” The network address for a PPTP server is not a secure network address because a client can communicate with the PPTP server without authorization, as I stated above in ¶ 11.

The Microsoft VPN Reference

66. Microsoft VPN is a compilation of various Microsoft documents. As identified by the Request at page 52, Microsoft VPN discloses PPTP connections for remote users to access a corporate network. Microsoft VPN discloses at page 32, creating an IP address or host name of a corporate office “VPN” server. Microsoft VPN also discloses a conventional DNS structure at pages 64-66. Microsoft VPN, however, has not been shown to teach or disclose a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

67. The Request asserts that the hostname associated with a PPTP server, which is used to establish PPTP connections between a client and a target computer is a secure domain name. This is incorrect. A secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and target, as I stated above in ¶¶ 9-12.

Control No.: 95/001,270
Declaration of Jason Nieh, Ph.D.

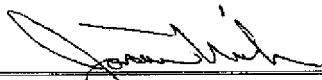
68. The Request, at page 54, also alleges that, since Microsoft VPN discloses a conventional DNS, which resolves domain names, a DNS request for the IP address for a PPTP server renders the traditional DNS a secure domain name service. A conventional DNS is not transformed into a secure domain name service merely by resolving a request for the IP address of a server which is used to establish PPTP connections. As I stated in ¶¶ 9-12, above, disclosure of a conventional DNS does not disclose a secure domain name service, as recited in claims 1, 17, and 33.

69. The Request, at page 54, also alleges that the network address of a PPTP server, which enables a PPTP connection between a client and a target, is a “secure computer network address.” The network address for a PPTP server is not a secure network address because a client can communicate with the PPTP server without authorization, as I stated above in ¶ 11. Further, because it does not have a secure computer network address, its domain name cannot be secure domain name.

Truth and Accuracy of Statements

70. I further 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 willful false statements or the like may jeopardize the validity of the application or any patent issuing thereon.

Signed at New York, New York this 19 th day of April, 2010.



Jason Nieh, Ph.D.

BST99 1647647-6.077580.0090

EXHIBIT A

Jason Nieh - Curriculum Vitae

Columbia University
Department of Computer Science
1214 Amsterdam Ave. MC0401
New York, NY 10027-7003

Office: (212) 939-7160
Fax: (212) 666-0140
nieh@cs.columbia.edu
<http://www.cs.columbia.edu/~nieh>

RESEARCH INTERESTS

Mobile computing, operating systems, distributed systems, thin-client computing, web and multimedia systems, and performance evaluation.

EDUCATION

Ph.D. Electrical Engineering, **Stanford University**, Stanford, CA, June 1999. Dissertation: "The Design, Implementation, and Evaluation of SMART: A Scheduler for Multimedia Applications", advisor Monica S. Lam.

M.S. Electrical Engineering, **Stanford University**, Stanford, CA, June 1990.

B.S. Electrical Engineering, **Massachusetts Institute of Technology**, Cambridge, MA, June 1989. Dissertation: "Using Special-Purpose Computing to Examine Chaotic Behavior in Nonlinear Mappings", advisor Gerald J. Sussman.

HONORS

IBM Faculty Award, 2004, 2006, 2008.

LISA Best Student Paper Award, 2005.

Sigma Xi Young Investigator Award, 2004. Awarded biennially to one individual for scientific achievement in the physical sciences and engineering. First computer scientist to receive this national award.

ACM MobiCom Best Student Paper Award, 2004.

Distinguished Faculty Teaching Award, Columbia Engineering School Alumni Association, 2004. Awarded to the top two instructors in the School of Engineering and Applied Science at Columbia University.

IBM Shared University Research (SUR) Award, 2000, 2004.

IBM Performance Modeling and Analysis PIC Best Paper Award, 2004.

Department of Energy Early Career Principal Investigator Award, 2003.

National Science Foundation Faculty Early Career Development (CAREER) Award, 2001.

Sun Microsystems SAM Award, 1994.

GE Foundation Fellowship, 1989.

California Microelectronics Fellowship, 1989 (declined).

AT&T Engineering Scholarship, 1986-1989.

Member, Eta Kappa Nu, 1988.

Member, Sigma Xi, 1988.

Member, Tau Beta Pi, 1988.

PROFESSIONAL EXPERIENCE

Associate Professor of Computer Science, **Columbia University**, New York, NY, 2003 - present.

Director, Network Computing Laboratory, **Columbia University**, New York, NY, 2000 - present.

Founder, **Guitar Notes, Inc.**, New York, NY, 1996 - present.

Expert Witness, *01 Communique Laboratory v. Citrix Systems*, **Goodwin Procter**, Boston, MA, 2006 - 2008.

Chief Scientist, **DeskTone**, Chelmsford, MA, 2006 - 2007.

1st Scholar in Residence, **VMware**, Palo Alto, CA, 2006 - 2007.

Consultant, *Rothschild Trust v. Citrix Systems*, **Goodwin Procter**, Boston, MA, 2006.

Technical Advisor, *Microsoft Consent Decree*, **States of NY, OH, IL, KY, LA, MD, MI, NC, and WI**, 2003 - 2006.

Expert Witness, *Cox v. Microsoft*, **Milberg Weiss Bershad and Schulman**, New York, NY, 2005 - 2006.

Assistant Professor of Computer Science, **Columbia University**, New York, NY, 1999 - 2003.

Chairman of Technology Office and Director, **TrueMetrix**, New York, NY, 1999 - 2000.

Technical Consultant, **Vertex Management**, Redwood Shores, CA, 1996 - 1997.

Academic Consultant, **Sun Microsystems Laboratories**, Mountain View, CA, 1993 - 1998.

Research Assistant, Dept. of Electrical Engineering, **Stanford University**, Stanford, CA, 1990 - 1998.

Summer Institute in Parallel Computing, **Argonne National Laboratories**, Argonne, IL, 1991.

Undergraduate Researcher, **Massachusetts Institute of Technology**, Cambridge, MA, 1987 - 1989.

Summer Intern, **AT&T Bell Laboratories**, Lincroft, Middletown, and Murray Hill, NJ, 1986 - 1988.

RESEARCH SUPPORT (all co-principal investigators at Columbia University unless otherwise noted)

1. Principal Investigator, "TC:Small: Exploiting Software Elasticity for Automatic Software Self-Healing", Trustworthy Computing Program, **National Science Foundation**, CNS-0914845, \$450,000, Sept. 1, 2009 - Aug. 31, 2012, with Angelos D. Keromytis.
2. Co-Principal Investigator, "CSR: Medium: Guanyin: a Thousand hands with a Thousand eyes for Distributed Software Checking", Computer Systems Research Program, **National Science Foundation**, CNS-0905246, \$1,102,000, Sept. 1, 2009 - Aug. 31, 2013, with Junfeng Yang and Gail E. Kaiser.
3. Principal Investigator, "Google Desktop Meets DejaView: Display-Centric Desktop Search", Google Research Award, **Google**, \$70,000, Sept. 1, 2009 - Aug. 31, 2010, with Luis Gravano.
4. Principal Investigator, "Android G1 Dev Phone Equipment Grant", **Google**, \$23,940, Sept. 2009.
5. Principal Investigator, "DejaView / Android Development", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$20,000, Sept. 1, 2009 - Feb. 28, 2010.
6. Principal Investigator, "GOALI Supplement to CSR-VSM: Autonomic Mechanisms for Reducing System Downtime due to Maintenance and Upgrades", Grant Opportunities for Academic Liaison with Industry Program, **National Science Foundation**, CNS-0950434, \$66,675, Sept. 1, 2009 - Aug. 31, 2010.
7. Principal Investigator, "CIFellow: Michael Hines", Subaward through Computing Community Consortium and Computing Research Association, **National Science Foundation**, CNS-0937060, \$140,000, Sept. 1, 2009 - Aug. 31, 2010.
8. Principal Investigator, "An Open Standard for Advanced Display and Application Remoting", IBM Faculty Award, **IBM Research**, \$20,000, July 1, 2008 - June 30, 2009.
9. Principal Investigator, "Remote 3D Gaming Research", **Deutsche Telekom AG, Laboratories**, \$70,930, Sept. 1, 2007 - Aug. 31, 2008.
10. Principal Investigator, "Virtualization Mechanisms for Security", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$38,559, July 1, 2007 - June 30, 2008.
11. Principal Investigator, "Virtualization Curriculum Equipment Grant", **VMware**, \$40,000, Sept. 2007.
12. Co-Principal Investigator, "CSR-VSM: Autonomic Mechanisms for Reducing System Downtime due to Maintenance and Upgrades", Computer Systems Research Program, **National Science Foundation**, CNS-0717544, \$350,000, Aug. 1, 2007 - July 31, 2009, with Gail E. Kaiser.

13. Co-Principal Investigator, "Autonomic Recovery of Enterprise-Wide Systems After Attack or Failure with Forward Correction", Multidisciplinary University Research Initiative (MURI), **Air Force Office of Scientific Research (AFOSR)**, USAF/AFRL FA9550-07-1-0527, \$4,826,940, May 1, 2007 - Apr. 30, 2012, with Anup K. Ghosh (George Mason University), Sushil Jajodia, (George Mason University), Angelos D. Keromytis, Salvatore J. Stolfo, and Peng Liu (Pennsylvania State University).
14. Principal Investigator, "Thin-Client Computing Research", **Advanced Micro Devices**, \$50,000, Jan. 1, 2007 - Dec. 31, 2007.
15. Principal Investigator, "Secure Isolation Mechanisms for Untrusted Network Applications", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$10,000, July 1, 2006 - June 30, 2007.
16. Co-Principal Investigator, "Security Escorts For Not-Yet Trusted Software", Small Business Technology Transfer Research Program (STTR), **Office of the Secretary of Defense**, O064-SP2-1001, \$99,981, Aug. 15, 2006 - May 15, 2007, with Charles Earl (Stottler Henke Associates).
17. Principal Investigator, "Virtualization Mechanisms for Security", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$38,559, July 1, 2006 - June 30, 2007.
18. Principal Investigator, "An Application Streaming Service for Ubiquitous Computing Access", IBM Faculty Award, **IBM Research**, \$20,000, July 1, 2006 - June 30, 2007.
19. Principal Investigator, "BPC Supplement to ITR: Secure Remote Computing Services", Broadening Participation in Computing Program, **National Science Foundation**, CNS-0543869, \$133,565, Sept. 15, 2005 - Sept. 14, 2007.
20. Principal Investigator, "US-Japan Cyber Trust Supplement to ITR: Secure Remote Computing Services", Cyber Trust Program, **National Science Foundation**, CNS-0535343, \$77,280, July 1, 2005 - June 30, 2007.
21. Principal Investigator, "Secure Isolation Mechanisms for Untrusted Network Applications", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$12,500, July 1, 2005 - June 30, 2006.
22. Principal Investigator, "Sun Ray Software Performance", Collaborative Research Program, **Sun Microsystems**, \$45,142, Feb. 2005.
23. Principal Investigator, "ITR: Secure Remote Computing Services", Information Technology Research (ITR) for National Priorities Program, **National Science Foundation**, CNS-0426623, \$1,200,000, Sept. 15, 2004 - Aug. 31, 2009, with Gail E. Kaiser and Angelos D. Keromytis.
24. Principal Investigator, "Secure Isolation Mechanisms for Untrusted Network Applications", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$12,500, July 1, 2004 - June 30, 2005.
25. Principal Investigator, "Secure Isolation and Transparent Migration of Legacy Applications", IBM Faculty Award, **IBM Research**, \$40,000, July 1, 2004 - June 30, 2005.
26. Principal Investigator, "Secure Isolation and Migration of Linux Applications", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$70,000, Apr. 19, 2004 - June 30, 2004.
27. Principal Investigator, "Linux Virtualization Phase I", IBM Shared University Research (SUR) Award, **IBM Research**, \$503,027, Mar. 2004.
28. Principal Investigator, "Migration Mechanisms for Large-Scale Parallel Applications", Early Career Principal Investigator Program in Applied Mathematics, Collaboratory Research, Computer Science, and High-Performance Networks, Office of Science, **US Department of Energy**, \$299,589, Aug. 15, 2003 - Aug. 14, 2007.
29. Principal Investigator, "Sun Microsystems Equipment Grant", Collaborative Research Program, **Sun Microsystems**, \$6,195, July 2003.
30. Principal Investigator, "Network Virtualization Mechanisms for Mobile Communication", Networking Research Program, **National Science Foundation**, ANI-0240525, \$249,999, June 1, 2003 - May 31, 2007.

31. Principal Investigator, "Apple Computer Powerbook Award", Apple Developer Connection and Hardware Seed Program, **Apple Computer**, \$7,433, May 2003.
32. Principal Investigator, "ITR: An Experimental Study of Thin-Client Computing Architectures", Information Technology Research (ITR) Program, **National Science Foundation**, CCR-0219943, \$250,000, Sept. 1, 2002 - July 31, 2007.
33. Senior Personnel, "Pervasive Pixels", CISE Research Infrastructure Program, **National Science Foundation**, EIA-0202063, \$1,485,098, Sept. 1, 2002 - Aug. 31, 2007, with Henning Schulzrinne, Steven K. Feiner, Gail E. Kaiser, John R. Kender, Kathleen R. McKeown, Peter K. Allen, Angelos D. Keromytis, Shree K. Nayar, William Noble, Steven M. Nowick, and Kenneth A. Ross.
34. Principal Investigator, "Migration Mechanisms for Autonomic Computing", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$70,000, July 1, 2002 - June 30, 2003.
35. Principal Investigator, "Inferring Mean Client Response Time at the Web Server", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$25,000, Apr. 1, 2002 - June 30, 2002.
36. Co-Principal Investigator, "The Columbia Hot Spot Rescue Service", Advanced Networking Infrastructure and Research (ANIR) Special Projects in Networking Program, **National Science Foundation**, ANI-0117738, \$1,399,999, Sept. 15, 2001 - Aug. 30, 2006, with Edward G. Coffman, Predrag R. Jelenkovic, Dan Rubenstein, and Henning Schulzrinne.
37. Principal Investigator, "Scalability Issues in Linux", Collaborative Research Program, **IBM Linux Technology Center**, \$33,029, July 1, 2001 - June 30, 2002.
38. Principal Investigator, "Thin-Client Benchmarking", **National Semiconductor**, \$25,000, July 1, 2001 - June 30, 2002.
39. Principal Investigator, "Server-Based Computing Technologies for Application Service Providers", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$75,000, July 1, 2001 - June 30, 2002.
40. Principal Investigator, "Scalable Linux Cluster Utilities", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, \$50,000, Apr. 16, 2001 - June 30, 2001.
41. Principal Investigator, "CAREER: Delivering Computational Services over the Internet", Faculty Early Career Development (CAREER) Award, Operating Systems and Compilers Program, **National Science Foundation**, CCR-0093047, \$250,000, Feb. 15, 2001 - Feb. 28, 2007.
42. Principal Investigator, "Scalable Linux Cluster Computer Utilities", IBM Shared University Research (SUR) Award, **IBM Research**, \$128,162, Dec. 2000.
43. Co-Principal Investigator, "Adaptive Internet Interactive Team Video", Experimental Systems Program, **National Science Foundation**, EIA-0071954, \$1,590,000, Sept. 15, 2000 - Sept. 30, 2004, with John R. Kender and Gail E. Kaiser.
44. Principal Investigator, "Columbia University Computer Utility", Collaborative Research Program, **Sun Microsystems**, \$51,178, Sept. 1, 2000 - Oct. 31, 2001.
45. Principal Investigator, "Lucent Grant in Science and Engineering", University Program, **Lucent Technologies**, \$20,000, July 2000.
46. Principal Investigator, "Sun Microsystems Equipment Grant", Collaborative Research Program, **Sun Microsystems**, \$83,562, Dec. 1999.
47. Co-Principal Investigator, "Microsoft Research and Education Grant", Microsoft University Program, **Microsoft Research**, \$1,208,163, July 1, 1999 - June 30, 2001, with Kathleen R. McKeown, Luis Gravano, John R. Kender, Andrew Kosoresow, Shree K. Nayar, and Henning Schulzrinne.

PUBLICATIONS

Most of these papers are available online at <http://www.ncl.cs.columbia.edu/publications>.

REFEREED JOURNAL ARTICLES

1. Albert M. Lai, Justin B. Starren, David R. Kaufman, Eneida A. Mendonca, Walter Palmas, Jason Nieh, and Steven Shea, "The Remote Patient Education in a Telemedicine Environment Architecture (REPETE)", *Telemedicine and e-Health*, 14(5), May 2008, pp. 355-361.
2. Albert Lai and Jason Nieh, "On the Performance of Wide-Area Thin-Client Computing", *ACM Transactions on Computer Systems (TOCS)*, 24(2), May 2006, pp. 175-209.
3. David P. Olshefski, Jason Nieh, and Dakshi Agarwal, "Using Certes to Infer Client Response Times at the Web Server", *ACM Transactions on Computer Systems (TOCS)*, 22(1), Feb. 2004, pp. 49-93. (2004 Best Paper, Performance Modeling and Analysis PIC, IBM Research; nominated for the 2004 Pat Goldberg Memorial Best Paper Awards in Computer Science, Electrical Engineering and Mathematics)
4. Jason Nieh and Monica S. Lam, "A SMART Scheduler for Multimedia Applications", *ACM Transactions on Computer Systems (TOCS)*, 21(2), May 2003, pp. 117-163.
5. Jason Nieh, S. Jae Yang, and Naomi Novik, "Measuring Thin-Client Performance Using Slow-Motion Benchmarking", *ACM Transactions on Computer Systems (TOCS)*, 21(1), Feb. 2003, pp. 87-115.

REFEREED CONFERENCE PAPERS

6. Shaya Potter and Jason Nieh, "Apiary: Easy-to-use Desktop Application Fault Containment on Commodity Operating Systems", *Proceedings of the 2010 USENIX Annual Technical Conference (USENIX 2010)*, Boston, MA, June 23-25, 2010. (17% accepted, 24/141)
7. Oren Laadan, Nicolas Viennot, and Jason Nieh, "Transparent, Lightweight Application Execution Replay on Commodity Multiprocessor Operating Systems", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2010)*, New York, NY, June 14-18, 2010. (16% accepted, 29/184)
8. Haoqiang Zheng and Jason Nieh, "RSIO: Automatic User Interaction Detection and Scheduling", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2010)*, New York, NY, June 14-18, 2010. (16% accepted, 29/184)
9. Oren Laadan, Dan Phung, and Jason Nieh, "Operating System Virtualization: Practice and Experience", *Proceedings of the 3rd Annual Haifa Experimental Systems Conference (SYSTOR 2010)*, Haifa, Israel, May 24-26, 2010. (58% accepted, 18/31)
10. Oren Laadan, Jason Nieh, and Nicolas Viennot, "Teaching Operating Systems Using Virtual Appliances and Distributed Version Control", *Proceedings of the 41st ACM Technical Symposium on Computer Science Education (SIGCSE 2010)*, Milwaukee, WI, Mar. 10-13, 2010, pp. 480-484. (34% accepted, 103/303)
11. Shaya Potter, Ricardo Baratto, Oren Laadan, Leonard Kim, and Jason Nieh, "MediaPod: A Personalized Multimedia Desktop In Your Pocket", *Proceedings of the 11th IEEE International Symposium on Multimedia (ISM 2009)*, San Diego, CA, Dec. 14-16, 2009, pp. 219-226. (20% accepted, 30/153)
12. Alex Sherman, Jason Nieh, and Clifford Stein, "FairTorrent: Bringing Fairness to Peer-to-Peer Systems", *Proceedings of the 5th ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT 2009)*, Rome, Italy, Dec. 1-4, 2009, pp. 133-144. (17% accepted, 29/170, one of the top three papers submitted, fast tracked to *IEEE/ACM Transactions on Networking*)
13. Shaya Potter, Steven M. Bellovin, and Jason Nieh, "Two-Person Control Administration: Preventing Administration Faults Through Duplication", *Proceedings of the 23rd Large Installation System Administration Conference (LISA 2009)*, Baltimore, MD, Nov. 1-6, 2009, pp. 15-27. (32% accepted, 12/38)
14. Shaya Potter, Ricardo Baratto, Oren Laadan, and Jason Nieh, "GamePod: Persistent Gaming Sessions on Pocketable Storage Devices", *Proceedings of the 3rd International Conference on Mobile Ubiquitous Computing, Systems, Services, and Technologies (UBICOMM 2009)*, Sliema, Malta, Oct. 11-16, 2009. (32% accepted)

15. Angelos Stavrou, Ricardo Baratto, Angelos Keromytis, and Jason Nieh, "A2M: Access-Assured Mobile Desktop Computing", *Proceedings of the 12th Information Security Conference (ISC 2009)*, Pisa, Italy, Sept. 7-9, 2009, pp. 186-201. (28% accepted, 29/105)
16. Alex Sherman, Angelos Stavrou, Jason Nieh, Angelos Keromytis, and Clifford Stein, "Adding Trust to P2P Distribution of Paid Content", *Proceedings of the 12th Information Security Conference (ISC 2009)*, Pisa, Italy, Sept. 7-9, 2009, pp. 459-474. (28% accepted, 29/105)
17. Haoqiang Zheng and Jason Nieh, "WARP: Enabling Fast CPU Scheduler Development and Evaluation", *Proceedings of the 2009 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS 2009)*, Boston, MA, Apr. 19-21, 2009, pp. 101-112. (28% accepted, 24/86)
18. Stelios Sidiroglou, Oren Laadan, Carlos R. Pérez, Nicolas Viennot, Jason Nieh, and Angelos D. Keromytis, "ASSURE: Automatic Software Self-healing Using REscue points", *Proceedings of the 14th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2009)*, Washington, DC, Mar. 7-11, 2009, pp. 37-48. (26% accepted, 29/113)
19. Shaya Potter, Jason Nieh, and Matthew Selsky, "Secure Isolation of Untrusted Legacy Applications", *Proceedings of the 21st Large Installation System Administration Conference (LISA 2007)*, Dallas, TX, Nov. 11-16, 2007, pp. 117-130. (40% accepted, 22/55)
20. Albert Lai, Jason Nieh, and Justin Starren, "REPETE2: A Next Generation Home Telemedicine Architecture", *Proceedings of the American Medical Informatics Association (AMIA) 2007 Annual Symposium*, Chicago, IL, Nov. 10-14, 2007, p. 1020. (poster paper)
21. Oren Laadan, Ricardo Baratto, Shaya Potter, Dan Phung, and Jason Nieh, "DejaView: A Personal Virtual Computer Recorder", *Proceedings of the 21st ACM Symposium on Operating Systems Principles (SOSP 2007)*, Stevenson, WA, Oct. 14-17, 2007, pp. 279-292. (19% accepted, 25/130)
22. Oren Laadan and Jason Nieh, "Transparent Checkpoint/Restart of Multiple Processes on Commodity Operating Systems", *Proceedings of the 2007 USENIX Annual Technical Conference (USENIX 2007)*, Santa Clara, CA, June 17-22, 2007, pp. 323-336. (21% accepted, 24/117)
23. Stelios Sidiroglou, Oren Laadan, Angelos D. Keromytis, and Jason Nieh, "Using Rescue Points to Navigate Software Recovery (Short Paper)", *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP 2007)*, Oakland, CA, May 20-23, 2007, pp. 273-280. (short paper, 12% accepted, 28/243, 8 short papers, 20 full papers)
24. Joeng Kim, Ricardo Baratto, and Jason Nieh, "An Application Streaming Service for Mobile Handheld Devices", *Proceedings of the IEEE International Conference on Services Computing (SCC 2006)*, Chicago, IL, Sept. 18-22, 2006, pp. 323-326. (short paper, 13% accepted, 22 short papers, 29 full papers)
25. Shaya Potter and Jason Nieh, "Highly Reliable Mobile Desktop Computing in Your Pocket", *Proceedings of the IEEE Computer Society Signature Conference on Software Technology and Applications (COMPSAC 2006)*, Chicago, IL, Sept. 18-21, 2006, pp. 247-254. (29% accepted, 54/184)
26. Bogdan Caprita, Jason Nieh, and Clifford Stein, "Grouped Distributed Queues: Distributed Queue, Proportional Share Multiprocessor Scheduling", *Proceedings of the 25th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2006)*, Denver, CO, July 23-26, 2006, pp. 72-81. (22% accepted, 30/136)
27. David P. Olshefski and Jason Nieh, "Understanding the Management of Client Perceived Pageview Response Time", *Proceedings of the Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS/Performance 2006)*, St. Malo, France, June 26-30, 2006, pp. 240-251. (14% accepted, 30/217)
28. Joeng Kim, Ricardo Baratto, and Jason Nieh, "pTHINC: A Thin-Client Architecture for Mobile Wireless Web", *Proceedings of the 15th International World Wide Web Conference (WWW2006)*, Edinburgh, Scotland, May 23-26, 2006, pp. 143-152. (10% accepted, 70/673)
29. Shaya Potter and Jason Nieh, "Reducing Downtime Due to System Maintenance and Upgrades", *Proceedings of the 19th Large Installation System Administration Conference (LISA 2005)*, San Diego, CA, Dec. 4-9, 2005, pp. 47-62. (46% accepted, 24/52, Best Student Paper Award)
30. Bogdan Caprita, Jason Nieh, and Wong Chun Chan, "Group Round Robin: Improving the Fairness and Complexity of Packet Scheduling", *Proceedings of the 1st ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2005)*, Princeton, NJ, Oct. 26-28, 2005, pp. 29-40. (32% accepted, 23/71)

31. Ricardo Baratto, Leonard Kim, and Jason Nieh, "THINC: A Virtual Display Architecture for Thin-Client Computing", *Proceedings of the 20th ACM Symposium on Operating Systems Principles (SOSP 2005)*, Brighton, United Kingdom, Oct. 23-26, 2005, pp. 277-290. (13% accepted, 20/155)
32. Oren Laadan, Dan Phung, and Jason Nieh, "Transparent Checkpoint-Restart of Distributed Applications on Commodity Clusters", *Proceedings of the 2005 IEEE International Conference on Cluster Computing (Cluster 2005)*, Boston, MA, Sept. 27-30, 2005, 13 pages. (35% accepted, 45/130)
33. Shaya Potter and Jason Nieh, "AutoPod: Unscheduled System Updates with Zero Data Loss", *Proceedings of the 2nd IEEE International Conference on Autonomic Computing (ICAC 2005)*, Seattle, WA, June 13-16, 2005, pp. 367-368. (poster paper, 38% accepted, 64/170, 39 poster papers, 25 full papers)
34. Shaya Potter and Jason Nieh, "WebPod: Persistent Web Browsing Sessions with Pocketable Storage Devices", *Proceedings of the 14th International World Wide Web Conference (WWW2005)*, Chiba, Japan, May 10-14, 2005, pp. 603-612. (14% accepted, 77/550, nominated for Best Presentation Award)
35. Bogdan Caprita, Wong Chun Chan, Jason Nieh, Clifford Stein, and Haoqiang Zheng, "Group Ratio Round Robin: O(1) Proportional Share Scheduling for Uniprocessor and Multiprocessor Systems", *Proceedings of the 2005 USENIX Annual Technical Conference (USENIX 2005)*, Anaheim, CA, Apr. 10-15, 2005, pp. 337-352. (20% accepted, 24/118)
36. Jason Nieh and Chris Vaill, "Experiences Teaching Operating Systems Using Virtual Platforms and Linux", *Proceedings of the 36th ACM Technical Symposium on Computer Science Education (SIGCSE 2005)*, St. Louis, MO, Feb. 23-27, 2005, pp. 520-524. (32% accepted, 104/330)
37. Angelos Stavrou, Angelos D. Keromytis, Jason Nieh, Vishal Misra, and Dan Rubenstein, "MOVE: An End-to-End Solution To Network Denial of Service", *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS 2005)*, San Diego, CA, Feb. 2-4, 2005, pp. 81-96. (13% accepted, 16/124)
38. David P. Olshefski, Jason Nieh, and Erich Nahum, "ksniffer: Determining the Remote Client Perceived Response Time from Live Packet Streams", *Proceedings of the 6th Symposium on Operating System Design and Implementation (OSDI 2004)*, San Francisco, CA, Dec. 6-8, 2004, pp. 333-346. (14% accepted, 27/193)
39. Ricardo Baratto, Shaya Potter, Gong Su, and Jason Nieh, "MobiDesk: Mobile Virtual Desktop Computing", *Proceedings of the 10th International Conference on Mobile Computing and Networking (MobiCom 2004)*, Philadelphia, PA, Sept. 29-Oct. 1, 2004, pp. 1-15. (8% accepted, 26/327, Best Student Paper Award)
40. Albert Lai, Jason Nieh, Andrew Laine, and Justin Starren, "Remote Display Performance for Wireless Healthcare Computing", *Proceedings of the 11th World Conference on Medical Informatics (Medinfo 2004)*, San Francisco, CA, Sept. 7-11, 2004, pp. 1438-1442. (42% accepted, 300/711)
41. Albert Lai, Jason Nieh, Bhagyashree Bohra, Vijayarka Nandikonda, Abhishek P. Surana, and Suchita Varshneya, "Improving Web Browsing on Wireless PDAs Using Thin-Client Computing", *Proceedings of the 13th International World Wide Web Conference (WWW2004)*, New York, NY, May 17-22, 2004, pp. 143-154. (15% accepted, 74/506)
42. Erez Zadok, Jeffrey Osborn, Ariye Shater, Charles Wright, Kiran-Kumar Muniswamy-Reddy, and Jason Nieh, "Reducing Storage Management Costs via Informed User-Based Policies", *Proceedings of the 12th NASA / Twenty-first IEEE Conference on Mass Storage Systems and Technologies (MSST)*, College Park, MD, Apr. 13-16, 2004, pp. 193-198. (short paper, 43% accepted, 32/75, 14 short papers, 18 full papers)
43. Haoqiang Zheng and Jason Nieh, "SWAP: A Scheduler with Automatic Process Dependency Detection", *Proceedings of the 1st USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI 2004)*, San Francisco, CA, Mar. 29-31, 2004, pp. 183-196. (< 23% accepted, 27/120+)
44. Albert Lai, Jason Nieh, Andrew Laine, and Justin Starren, "Thin Client Performance for Remote 3-D Image Display", *Proceedings of the American Medical Informatics Association (AMIA) 2003 Annual Symposium*, Washington, DC, Nov. 8-12, 2003, p. 904. (poster paper)
45. S. Jae Yang, Jason Nieh, Shilpa Krishnappa, Aparna Mohla, and Mahdi Sajjadpour, "Web Browsing Performance of Wireless Thin-Client Computing", *Proceedings of the 12th International World Wide Web Conference (WWW2003)*, Budapest, Hungary, May 20-24, 2003, pp. 68-79. (< 13% accepted, 77/600+)
46. Steven Osman, Dinesh Subhraveti, Gong Su, and Jason Nieh, "The Design and Implementation of Zap: A System for Migrating Computing Environments", *Proceedings of the 5th Symposium on Operating System Design and Implementation (OSDI 2002)*, Boston, MA, Dec. 9-11, 2002, pp. 361-376. (18% accepted, 27/150)

47. Albert Lai and Jason Nieh, "Limits of Wide-Area Thin-Client Computing", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2002)*, Marina del Rey, CA, June 15-19, 2002, pp. 228-239. (13% accepted, 23/170)
48. David P. Olshefski, Jason Nieh, and Dakshi Agarwal, "Inferring Client Response Times at the Web Server", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2002)*, Marina del Rey, CA, June 15-19, 2002, pp. 160-171. (13% accepted, 23/170)
49. S. Jae Yang, Jason Nieh, Matthew Selsky, and Nikhil Tiwari, "The Performance of Remote Display Mechanisms for Thin-Client Computing", *Proceedings of the 2002 USENIX Annual Technical Conference (USENIX 2002)*, Monterey, CA, June 10-15, 2002, pp. 131-146. (23% accepted, 25/107)
50. Fei Li and Jason Nieh, "Optimal Linear Interpolation Coding for Server-Based Computing", *Proceedings of the IEEE International Conference on Communications (ICC) 2002*, New York, NY, Apr. 28-May 2, 2002, pp. 2542-2546. (42% accepted, 655/1568)
51. Fei Li and Jason Nieh, "Low-complexity Interpolation Coding for Server-Based Computing", *Proceedings of the Data Compression Conference (DCC) 2002*, Snowbird, UT, Apr. 2-4, 2002, p. 461. (poster paper)
52. Jason Nieh, Chris Vaill, and Hua Zhong, "Virtual-Time Round-Robin: An O(1) Proportional Share Scheduler", *Proceedings of the 2001 USENIX Annual Technical Conference (USENIX 2001)*, Boston, MA, June 25-30, 2001, pp. 245-259. (29% accepted, 24/82, nominated for Best Paper Award)
53. S. Jae Yang, Jason Nieh, and Naomi Novik, "Measuring Thin-Client Performance Using Slow-Motion Benchmarking", *Proceedings of the 2001 USENIX Annual Technical Conference (USENIX 2001)*, Boston, MA, June 25-30, 2001, pp. 35-49. (29% accepted, 24/82)
54. Erez Zadok, Johan M. Andersen, Ion Badulescu, and Jason Nieh, "Fast Indexing: Support for Size-Changing Algorithms in Stackable File Systems", *Proceedings of the 2001 USENIX Annual Technical Conference (USENIX 2001)*, Boston, MA, June 25-30, 2001, pp. 289-304. (29% accepted, 24/82)
55. Erez Zadok and Jason Nieh, "FiST: A Language for Stackable File Systems", *Proceedings of the 2000 USENIX Annual Technical Conference (USENIX 2000)*, San Diego, CA, June 18-23, 2000, pp. 55-70. (30% accepted; 27/90)
56. Jason Nieh and Monica S. Lam, "The Design, Implementation and Evaluation of SMART: A Scheduler for Multimedia Applications", *Proceedings of the 16th ACM Symposium on Operating Systems Principles (SOSP 1997)*, St. Malo, France, Oct. 5-8, 1997, pp. 184-197. (< 20% accepted, 23/110+)
57. Jason Nieh and Monica S. Lam, "SMART UNIX SVR4 Support for Multimedia Applications", *Proceedings of the IEEE International Conference on Multimedia Computing and Systems (ICMCS 1997)*, Ottawa, Ontario, Canada, June 3-6, 1997, pp. 404-414. (~35% accepted)
58. Jason Nieh and Monica S. Lam, "SMART: A Processor Scheduler for Multimedia Applications", *Proceedings of the 15th Symposium on Operating Systems Principles (SOSP 1995)*, Copper Mountain Resort, CO, Dec. 3-5, 1995, p. 233. (poster paper, 40% accepted, 33/82, 11 poster papers, 22 full papers)

REFEREED WORKSHOP PUBLICATIONS

59. Alex Sherman, Jason Nieh, and Clifford Stein, "Fair Distributed Scheduling Algorithm for a P2P System", *9th Workshop on Models and Algorithms for Planning and Scheduling Problems (MAPSP 2009)*, Abbey Rolduc, The Netherlands, June 29-July 3, 2009.
60. Alfred Aho, Angelos D. Keromytis, Vishal Misra, Jason Nieh, Kenneth A. Ross, and Yechiam Yemini, "FlowPuter: A Cluster Architecture Unifying Switch, Server and Storage Processing", *Proceedings of the 1st International Workshop on Data Processing and Storage Networking: Towards Grid Computing (DPSN 2004)*, Athens, Greece, May 14, 2004, pp. 2/1-2/7 (60% accepted, 6/10).
61. Angelos D. Keromytis, Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, and Sal Stolfo, "A Holistic Approach to Service Survivability", *Proceedings of the 2003 ACM Workshop on Survivable and Self-Regenerative Systems*, Fairfax, VA, Oct. 31, 2003, pp. 11-22. (38% accepted, 10/26)
62. Ed Coffman, Predrag Jelenkovic, Jason Nieh, Dan Rubenstein, and Henning Schulzrinne, "The Columbia Hotspot Rescue Service", *Internet2 Network Research Workshop Spring 2001*, Chicago, IL, Apr. 18-19, 2001.

63. Jason Nieh and S. Jae Yang, "Measuring the Multimedia Performance of Server-Based Computing", *Proceedings of the 10th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 2000)*, Chapel Hill, NC, June 26-28, 2000, pp. 55-64. (45% accepted, 32/70)
64. Jason Nieh and Monica S. Lam, "Multimedia on Multiprocessors: Where's the OS When You Really Need It?", *Proceedings of the 8th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 1998)*, Cambridge, UK, July 8-10, 1998, pp. 103-106. (45% accepted, 36/80)
65. Jason Nieh and Monica S. Lam, "Integrated Processor Scheduling for Multimedia", *Proceedings of the 5th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 1995)*, Durham, NH, Apr. 18-22, 1995, *Lecture Notes in Computer Science*, 1018, Springer-Verlag, pp. 215-218. (40% accepted, 40/101)
66. Jason Nieh, James G. Hanko, J. Duane Northcutt, and Gerard A. Wall, "SVR4 UNIX Scheduler Unacceptable for Multimedia Applications", *Proceedings of the 4th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 1993)*, Lancaster, United Kingdom, Nov. 3-5, 1993, *Lecture Notes in Computer Science*, 846, Springer-Verlag, pp. 35-48. (24% accepted, 24/100)
67. Jason Nieh and Marc Levoy, "Volume Rendering on Scalable Shared-Memory MIMD Architectures", *Proceedings of the Boston Workshop on Volume Visualization*, Boston, MA, Oct. 19-20, 1992, pp. 17-24.

INVITED BOOK CHAPTERS AND CONTRIBUTIONS

68. Albert Lai and Jason Nieh, "Web Content Delivery Using Thin-Client Computing", *Web Content Delivery*, ed. Samuel Chanson, Xueyan Tang, and Jianliang Xu, Springer, 2005, pp. 325-345.
69. Jason Nieh and Monica S. Lam, "The Design, Implementation and Evaluation of SMART: A Scheduler for Multimedia Applications", *Readings in Multimedia Computing and Networking*, ed. Kevin Jeffay and HongJiang Zhang, Morgan Kaufmann Publishers, 2002, pp. 506-519.

INVITED MAGAZINE ARTICLES

70. Shaya Potter and Jason Nieh, "Breaking the Ties that Bind: Process Isolation and Migration", *login*, USENIX Association, 30(6), Dec. 2005, pp. 14-17.
71. S. Jae Yang and Jason Nieh, "MetaFrame XP Extends the Citrix Platform", *PC Magazine*, Ziff-Davis Media, 21(9), May 7, 2002, p. 48.
72. Jason Nieh and Ozgur C. Leonard, "Examining VMware", *Dr. Dobb's Journal*, 315, Miller Freeman, San Mateo, CA, Aug. 2000, pp. 70-76.
73. S. Jae Yang and Jason Nieh, "Thin Is In", *PC Magazine*, 19(13), Ziff-Davis Media, July 1, 2000, p. 68.

INVITED CONFERENCE PAPERS

74. Kenneth Ocheltree, Steven Millman, David Hobbs, Martin McDonnell, Jason Nieh, and Ricardo Baratto, "Net2Display: A Proposed VESA Standard for Remoting Displays and I/O Devices over Networks", *Proceedings of the 2006 Americas Display Engineering and Applications Conference (ADEAC 2006)*, Atlanta, Georgia, Oct. 23-26, 2006.

OTHER PUBLICATIONS

75. Dinesh Subhraveti and Jason Nieh, "Record and Transplay: Partial Checkpointing for Replay Debugging", Technical Report CUCS-050-09, Dept. of Computer Science, Columbia University, Nov. 2009.
76. Shaya Potter and Jason Nieh, "Apiary: Easy-to-use Desktop Application Fault Containment on Commodity Operating Systems", Technical Report CUCS-034-09, Dept. of Computer Science, Columbia University, Aug. 2009.
77. Alex Sherman and Jason Nieh, "FairStream: Improving Peer-to-Peer Streaming Performance through Fairness", Technical Report CUCS-018-09, Dept. of Computer Science, Columbia University, Apr. 2009.
78. Nicolas Viennot, Oren Laadan, and Jason Nieh, "Transparent, Lightweight Application Execution Replay on Commodity Multiprocessor Operating Systems", Technical Report CUCS-017-09, Dept. of Computer Science, Columbia University, Apr. 2009.
79. Alex Sherman, Jason Nieh, and Cliff Stein, "FairTorrent: Bringing Fairness to Peer-to-Peer Systems", Technical Report CUCS-011-09, Dept. of Computer Science, Columbia University, Mar. 2009.

80. Shaya Potter and Jason Nieh, "Improving Virtual Appliance Management through Virtual Layered File Systems", Technical Report CUCS-008-08, Dept. of Computer Science, Columbia University, Jan. 2009.
81. Oren Laadan and Jason Nieh, "Operating System Virtualization: Practice and Experience", Technical Report CUCS-058-08, Dept. of Computer Science, Columbia University, Dec. 2008.
82. Leon L. Wu, Gail E. Kaiser, Jason Nieh, and Christian Murphy, "Deux: Autonomic Testing System for Operating System Upgrades", Technical Report CUCS-037-08, Dept. of Computer Science, Columbia University, Aug. 2008.
83. Alex Sherman, Jason Nieh, and Clifford Stein, "FairTorrent: Bringing Fairness to Peer-to-Peer Systems", Technical Report CUCS-029-08, Dept. of Computer Science, Columbia University, May 2008.
84. Haoqiang Zheng and Jason Nieh, "Automatic User Interaction Detection and Scheduling with RSIO", Technical Report CUCS-028-08, Dept. of Computer Science, Columbia University, May 2008.
85. Alex Sherman, Angelos Stavrou, Jason Nieh, and Clifford Stein, "Mitigating the Effect of Free-Riders in BitTorrent using Trusted Agents", Technical Report CUCS-005-08, Dept. of Computer Science, Columbia University, Jan. 2008.
86. Alex Sherman, Angelos Stavrou, Jason Nieh, Clifford Stein, and Angelos D. Keromytis, "Can P2P Replace Direct Download for Content Distribution?", Technical Report CUCS-020-07, Dept. of Computer Science, Columbia University, Mar. 2007.
87. Alex Sherman, Japinder Chawla, Jason Nieh, Clifford Stein, and Justin Sarma, "Aequitas: A Trusted P2P System for Paid Content Delivery", Technical Report CUCS-019-07, Dept. of Computer Science, Columbia University, Mar. 2007.
88. Shaya Potter and Jason Nieh, "Improving Virtual Appliances through Virtual Layered File Systems", Technical Report CUCS-003-07, Dept. of Computer Science, Columbia University, Jan. 2007.
89. Alex Sherman, Angelos Stavrou, Jason Nieh, Clifford Stein, and Angelos D. Keromytis, "A Case for P2P Delivery of Paid Content", Technical Report CUCS-042-06, Dept. of Computer Science, Columbia University, Nov. 2006.
90. Alex Sherman, Jason Nieh, and Yoav Freund, "Feasibility of Voice over IP on the Internet", Technical Report CUCS-027-06, Dept. of Computer Science, Columbia University, June 2006.
91. Jason Nieh and Chris Vaill, "Experiences Teaching Operating Systems Using Virtual Platforms and Linux", *ACM Operating Systems Review (OSR)*, 40(2), Apr. 2006, pp. 100-104. (Reprint from *Proceedings of the 36th ACM Technical Symposium on Computer Science Education*, Feb. 2005.)
92. Bogdan Caprita, Jason Nieh, and Clifford Stein, "Grouped Distributed Queues: Distributed Queue, Proportional Share Multiprocessor Scheduling", Technical Report CUCS-004-06, Dept. of Computer Science, Columbia University, Feb. 2006.
93. Jonathan Lennox, Henning Schulzrinne, Jason Nieh, and Ricardo A. Baratto, "Protocols for Application and Desktop Sharing", Internet Draft draft-lennox-avt-app-sharing, IETF, Dec. 2004. Work in progress.
94. Henning Schulzrinne, Jonathan Lennox, Jason Nieh, and Ricardo A. Baratto, "Sharing and Remote Access to Applications", Internet Draft draft-schulzrinne-mmusic-sharing, IETF, Sept. 2004. Work in progress.
95. Shaya Potter and Jason Nieh, "WebPod: Persistent Web Browsing Sessions with Pocketable Storage Devices", Technical Report CUCS-047-04, Dept. of Computer Science, Columbia University, Nov. 2004.
96. Bogdan Caprita, Wong Chun Chan, Jason Nieh, Clifford Stein, and Haoqiang Zheng, "Group Ratio Round Robin: O(1) Proportional Share Scheduling for Uniprocessor and Multiprocessor Systems", Technical Report CUCS-028-04, Dept. of Computer Science, Columbia University, July 2004.
97. Ricardo Baratto, Jason Nieh, and Leo Kim, "THINC: A Remote Display Architecture for Thin-Client Computing", Technical Report CUCS-027-04, Dept. of Computer Science, Columbia University, July 2004.
98. Ricardo Baratto, Shaya Potter, Gong Su, and Jason Nieh, "MobiDesk: Mobile Virtual Desktop Computing", Technical Report CUCS-014-04, Dept. of Computer Science, Columbia University, Mar. 2004.
99. Shaya Potter, Jason Nieh, and Dinesh Subhraveti, "Secure Isolation and Migration of Untrusted Legacy Applications", Technical Report CUCS-005-04, Dept. of Computer Science, Columbia University, Jan. 2004.
100. Angelos D. Keromytis, Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, and Sal Stolfo, "A Holistic Approach to Service Survivability", Technical Report CUCS-021-03, Dept. of Computer Science, Columbia University, July 2003.

101. Bogdan Caprita, Wong Chun Chan, and Jason Nieh, "Group Round Robin: Improving the Fairness and Complexity of Packet Scheduling", Technical Report CUCS-018-03, Dept. of Computer Science, Columbia University, June 2003.
102. Wong Chun Chan and Jason Nieh, "Group Ratio Round-Robin: An O(1) Proportional Share Scheduler", Technical Report CUCS-012-03, Dept. of Computer Science, Columbia University, Apr. 2003.
103. Haoqiang Zheng and Jason Nieh, "SWAP: A Scheduler With Automatic Process Dependency Detection", Technical Report CUCS-005-03, Dept. of Computer Science, Columbia University, Apr. 2003.
104. Erez Zadok, Jeffrey Osborn, Ariye Shater, Charles Wright, Kiran-Kumar Muniswamy-Reddy, and Jason Nieh, "Reducing Storage Management Costs via Informed User-Based Policies", Technical Report FSL-03-01, Dept. of Computer Science, Stony Brook University, Mar. 2003.
105. Ozgur Can Leonard, Jason Nieh, Erez Zadok, Jeffrey Osborn, Ariye Shater, and Charles Wright, "The Design and Implementation of Elastic Quotas: A System for Flexible File System Management", Technical Report CUCS-014-02, Dept. of Computer Science, Columbia University, June 2002.
106. Ed Coffman, Predrag Jelenkovic, Jason Nieh, and Dan Rubenstein, "The Columbia Hot Spot Rescue Service: A Research Plan", Technical Report EE2002-005-131, Dept. of Electrical Engineering, Columbia University, May 2002.
107. Gong Su and Jason Nieh, "Mobile Communication with Virtual Network Address Translation", Technical Report CUCS-003-02, Dept. of Computer Science, Columbia University, Feb. 2002.
108. Hua Zhong and Jason Nieh, "CRAK: Linux Checkpoint / Restart As a Kernel Module", Technical Report CUCS-014-01, Dept. of Computer Science, Columbia University, Nov. 2001.
109. Erez Zadok, Johan M. Andersen, Ion Badulescu, and Jason Nieh, "Performance of Size-Changing Algorithms in Stackable File Systems", Technical Report CUCS-023-00, Dept. of Computer Science, Columbia University, Nov. 2000.
110. Jason Nieh, S. Jae Yang and Naomi Novik, "A Comparison of Thin-Client Computing Architectures", Technical Report CUCS-022-00, Dept. of Computer Science, Columbia University, Nov. 2000.
111. Erez Zadok and Jason Nieh, "FiST: A Language for Stackable File Systems", Technical Report CUCS-034-99, Dept. of Computer Science, Columbia University, Dec. 1999.
112. Jason Nieh, "The Design, Implementation, and Evaluation of SMART: A Scheduler for Multimedia Applications", Ph.D. Thesis, Dept. of Electrical Engineering, Stanford University, June 1999.
113. Jason Nieh and Monica S. Lam, "The Design, Implementation and Evaluation of SMART: A Scheduler for Multimedia Applications", Technical Report CSL-TR-97-721, Computer Systems Laboratory, Stanford University, Apr. 1997.
114. Jason Nieh and Monica S. Lam, "The SMART Scheduler", Project Technical Report SML-96-0213, Sun Microsystems Laboratories, July 1996.
115. Jason Nieh and Monica S. Lam, "The Design of SMART: A Scheduler for Multimedia Applications", Technical Report CSL-TR-96-697, Computer Systems Laboratory, Stanford University, June 1996.
116. Jason Nieh, Monica S. Lam, and J. Duane Northcutt, "A Practical Unified Approach to Processor Scheduling", Project Technical Report SML-94-0488, Sun Microsystems Laboratories, Dec. 1994.
117. Jason Nieh and Marc Levoy, "Volume Rendering on Scalable Shared-Memory MIMD Architectures", Technical Report CSL-TR-92-537, Computer Systems Laboratory, Stanford University, Aug. 1992.
118. Brian LaMacchia and Jason Nieh, "The Standard Map Machine", AI Memo 1165, AI Laboratory, Massachusetts Institute of Technology, Sept. 1989.
119. Jason Nieh, "Using Special-Purpose Computing to Examine Chaotic Behavior in Nonlinear Mappings", AI Technical Report 1139, AI Laboratory, Massachusetts Institute of Technology, Sept. 1989.
120. Jason Nieh, "DMI Mode 3 Throughput Analysis", Technical Memorandum, AT&T Information Systems, Dec. 1987.
121. Jason Nieh, "Delay and Throughput", Memorandum for File, AT&T Information Systems, Oct. 1986.

SELECTED INVITED TALKS

Distinguished Lecture, School of Computing and Information Sciences, Florida International University, Miami, FL, Feb. 2009.

Keynote Speaker, VMAP Summit, VMworld 2008, Las Vegas, NV, Sept. 2008.

Invited External Speaker, IBM System Software Day, IBM Watson Research Center, Yorktown Heights, NY, Sept. 2008.

Bell Laboratories, Alcatel-Lucent, Murray Hill, NJ, Nov. 2007.

Keynote Panel, VMworld 2006, Los Angeles, CA, Nov. 2006.

ITL Colloquium, National Institute of Standards and Technology (NIST), Washington, DC, June 2005.

DARPA ISAT Meeting, Washington, DC, June 2005.

CERCS Colloquium, Georgia Institute of Technology, Atlanta, GA, May 2005.

Invited Talk, 2005 USENIX Annual Technical Conference, Anaheim, CA, Apr. 2005.

DCS Colloquium, Rutgers University, Rutgers, NJ, Feb. 2005.

Young Investigator Lecture, 2004 Sigma Xi Annual Meeting, Montreal, Quebec Canada, Nov. 2004.

URCS Seminar, University of Rochester, Rochester, NY, Nov. 2004.

Systems Design and Implementation / Laboratory for Computer Systems (SDI/LCS) Seminar, Carnegie Mellon University, Pittsburgh, PA, Oct. 2004.

OS-PIC, IBM Watson Research Center, Yorktown Heights, NY, Oct. 2003.

MIT Workshop on Streaming Systems, Dedham, MA, Aug. 2003.

Hewlett-Packard Laboratories, Palo Alto, CA, June 2002.

Panasonic Information and Networking Technologies Laboratory, Princeton, NJ, May 2001.

OS-PIC, IBM Watson Research Center, Yorktown Heights, NY, April 2001.

Telcordia, Morristown, NJ, Nov. 2000.

OS-PIC, IBM Watson Research Center, Yorktown Heights, NY, May 2000.

Digital Equipment Systems Research Center, Palo Alto, CA, May 1998.

Division of Engineering and Applied Sciences, Harvard University, Cambridge, MA, May 1998.

Dept. of Computer Science, Yale University, New Haven, CT, Apr. 1998.

Dept. of Computer Science, Brown University, Providence, RI, Apr. 1998.

Dept. of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL, Apr. 1998.

Dept. of Computer and Information Science, University of Pennsylvania, Philadelphia, PA, Apr. 1998.

Dept. of Computer Science, University of Toronto, Toronto, Ontario, Canada, Apr. 1998.

Dept. of Computer Science, New York University, New York, NY, Mar. 1998.

Dept. of Computer Science, Northwestern University, Evanston, IL, Mar. 1998.

Hewlett-Packard Laboratories, Palo Alto, CA, June 1997.

Computer Forum Annual Meeting, Stanford University, Stanford, CA, Mar. 1997.

Computer Science Colloquium, University of California at Santa Barbara, Santa Barbara, CA, Mar. 1997.

IEEE RTSS Workshop on Resource Allocation Problems in Multimedia Systems, Washington, DC, Dec. 1996.

Distributed Systems Seminar, Stanford University, Stanford, CA, Apr. 1994.

Sun Microsystems Laboratories, Mountain View, CA, Oct. 1993.

Hewlett-Packard Laboratories, Palo Alto, CA, Oct. 1992.

Scientific Visualization Seminar, NASA Ames Research Center, Mountain View, CA, Sept. 1992.

PROFESSIONAL ACTIVITIES

EDITORIAL BOARDS

- Member, Editorial Board, *IEEE Internet Computing*, 2008 - present.
- Guest Editor, Special Issue on Virtual Machines, *IEEE Pervasive Computing*, Oct.-Dec. 2009.
- Member, Editorial Board, *Computer Networks Journal (COMNET)*, 2006 - 2008.

CONFERENCE PROGRAM COMMITTEES

- Member, Program Committee, *30th Annual IEEE Conference on Computer Communications (Infocom 2011)*, Shanghai, China, Apr. 10-15, 2011.
- Member, Program Committee, *16th International Conference on Mobile Computing and Networking (MobiCom 2010)*, Chicago, IL, Sept. 20-24, 2010.
- Member, Program Committee, *International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2010)*, New York, NY, June 14-18, 2010.
- Member, Program Committee, *3rd Annual Haifa Experimental Systems Conference (SYSTOR 2010)*, Haifa, Israel, May 24-26, 2010.
- Member, Program Committee, *29th Annual IEEE Conference on Computer Communications (Infocom 2010)*, San Diego, CA, Mar. 15-19, 2010.
- Member, Program Committee, *8th USENIX Conference on File and Storage Technologies (FAST 2010)*, San Jose, CA, Feb. 23-26, 2010.
- Member, Program Committee, *2nd Workshop on Hot Topics in Software Upgrades (HotSWUp 2009)*, Orlando, FL, Oct. 2009.
- Member, Program Committee, *1st Workshop on Networking, Systems, and Applications for Mobile Handhelds (MobiHeld 2009)*, Barcelona, Spain, Aug. 17, 2009.
- Member, Program Committee, *2nd Workshop on Mobile Computing and Virtualization (MobiVirt 2009)*, Kraków, Poland, June 22, 2009.
- Co-Chair, Program Committee, *Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS / Performance 2009)*, Seattle, WA, June 15-19, 2009.
- Member, Program Committee, *28th Annual IEEE Conference on Computer Communications (Infocom 2009)*, Rio de Janeiro, Brazil, Apr. 19-25, 2009.
- Member, Program Committee, *2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE 2009)*, Washington, DC, Mar. 11-13, 2009.
- Co-Chair, Program Committee, *1st ACM Workshop on Virtual Machine Security (VMSec 2008)*, Fairfax, VA, Oct. 31, 2008.
- Member, Program Committee, *5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2008)*, Dublin, Ireland, July 21-25, 2008.
- Member, Program Committee, *1st Workshop on Mobile Computing and Virtualization (MobiVirt 2008)*, Breckenridge, CO, June 17, 2008.
- Member, Program Committee, *International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2008)*, Annapolis, MD, June 2-6, 2008.
- Member, Program Committee, *27th Annual IEEE Conference on Computer Communications (Infocom 2008)*, Phoenix, AZ, Apr. 13-18, 2008.
- Member, Program Committee, *VMworld 2007*, San Francisco, Sept. 11-13, 2007.
- Member, Program Committee, *13th International Conference on Mobile Computing and Networking (MobiCom 2007)*, Montreal, Quebec, Canada, Sept. 9-14, 2007.

Member, Program Committee, *2007 USENIX Annual Technical Conference (USENIX 2007)*, Santa Clara, CA, June 17-22, 2007.

Member, Program Committee, *International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2007)*, San Diego, CA, June 12-16, 2007.

Member, Program Committee, *2007 ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys 2007)*, Puerto Rico, June 11-14, 2007.

Vice Chair, Program Committee, *16th International World Wide Web Conference (WWW2007)*, Banff, Alberta, Canada, May 8-12, 2007.

Member, Program Committee, *12th International Conference on Mobile Computing and Networking (MobiCom 2006)*, Los Angeles, CA, Sept. 24-29, 2006.

Member, Program Committee, *2006 IEEE International Conference on Cluster Computing (Cluster 2006)*, Barcelona, Spain, Sept. 25-27, 2006.

Member, Program Committee, *2006 USENIX Annual Technical Conference (USENIX 2006)*, Boston, MA, May 30-June 3, 2006.

Deputy Vice Chair, Program Committee, *15th International World Wide Web Conference (WWW2006)*, Edinburgh, UK, May 22-26, 2006.

Member, Program Committee, *International Conference on E-business and Telecommunication Networks (ICETE 2005)*, Reading, UK, Oct. 3-7, 2005.

Member, Program Committee, *International Work Conference on Next Generation Web Services Practices (NWeSP 2005)*, Seoul, Korea, Aug. 23-26, 2005.

Member, Program Committee, *IASTED International Conference on Web Technologies, Applications and Services (WTAS 2005)*, Calgary, Canada, July 4-6, 2005.

Member, Program Committee, *International Conference on Communications, Circuits and Systems (ICCCAS 2005)*, Hong Kong, China, May 27-30, 2005.

Member, Program Committee, *2005 USENIX Annual Technical Conference (USENIX 2005)*, Anaheim, CA, Apr. 10-15, 2005.

Member and WiPs Chair, Program Committee, *6th Symposium on Operating System Design and Implementation (OSDI 2004)*, San Francisco, CA, Dec. 6-8, 2004.

Member, Program Committee, *Multimedia Interactive Protocols and Systems (MIPS 2004)*, Grenoble, France, Nov. 16-19, 2004.

Member, Program Committee, *2nd International Conference on Service Oriented Computing (ICSOC 2004)*, New York, NY, Nov. 15-19, 2004.

Co-Chair, Program Committee, *1st ACM Workshop on Operating System and Architectural Support for the On Demand IT Infrastructure (OASIS 2004)*, Boston, MA, Oct. 9, 2004.

Member, Program Committee, *33rd International Conference on Parallel Processing (ICPP 2004)*, Montreal, Canada, Aug. 13-19, 2004.

Member, Program Committee, *International Conference on Communications, Circuits and Systems (ICCCAS 2004)*, Chengdu, China, June 27-29, 2004.

Member, Program Committee, *Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS / PERFORMANCE 2004)*, New York, NY, June 12-16, 2004.

Deputy Vice Chair, Program Committee, *13th International World Wide Web Conference (WWW2004)*, New York, New York, May 17-22, 2004.

Member, Program Committee, *Multimedia Interactive Protocols and Systems (MIPS 2003)*, Napoli, Italy, Nov. 18-21, 2003.

Member, Program Committee, *13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2003)*, Monterey, CA, June 1-3, 2003.

Member, Program Committee, *12th International World Wide Web Conference (WWW2003)*, Budapest, Hungary, May 20-24, 2003.

Member, Program Committee, *Joint International Workshop on Interactive Distributed Multimedia Systems / Protocols for Multimedia Systems (IDMS / PROMS 2002)*, Coimbra, Portugal, Nov. 26-29, 2002.

Member, Program Committee, *16th International Conference on Supercomputing (ICS 2002)*, New York, NY, June 22-26, 2002.

Member, Program Committee, *1st Workshop on Self-Healing, Adaptive and Self-MANaged Systems (SHAMAN 2002)*, New York, NY, June 23, 2002.

Member, Program Committee, *2002 USENIX Annual Technical Conference (USENIX 2002)*, Monterey, CA, June 9-14, 2002.

Member, Program Committee, *12th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2002)*, Miami Beach, FL, May 12-14, 2002.

Member, Program Committee, *8th International Workshop on Interactive Distributed Multimedia Systems (IDMS 2001)*, Lancaster, UK, Sept. 4-7, 2001.

Co-Chair, Program Committee, *11th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2001)*, New York, NY, June 25-26, 2001.

Member, Program Committee, *1st New York Metro Area Networking Workshop (NYMAN 2001)*, Hawthorne, NY, Mar. 12, 2001.

Member, Program Committee, *10th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2000)*, Chapel Hill, NC, June 26-28, 2000.

Member, Program Committee, *9th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 1999)*, Basking Ridge, NJ, June 23-25, 1999.

CONFERENCE STEERING AND ORGANIZING COMMITTEES

Member, Steering Committee, *15th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2005)*, Skamania, WA, June 12-14, 2005.

Local Organization Co-Chair, Organizing Committee, *2nd International Conference on Service Oriented Computing (ICSOC 2004)*, New York, NY, Nov. 15-19, 2004.

Co-Chair, Organizing Committee, *1st ACM Workshop on Operating System and Architectural Support for the On Demand IT Infrastructure (OASIS 2004)*, Boston, MA, Oct. 9, 2004.

Member, Steering Committee, *14th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2004)*, Cork, Ireland, June 16-18, 2004.

Publicity Chair, Organizing Committee, *Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS / PERFORMANCE 2004)*, New York, NY, June 12-16, 2004.

Member, Steering Committee, *13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2003)*, Monterey, CA, June 1-3, 2003.

University Liaison, Organizing Committee, *16th International Conference on Supercomputing (ICS 2002)*, New York, NY, June 22-26, 2002.

Member, Steering Committee, *12th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2002)*, Miami Beach, FL, May 12-14, 2002.

Co-Chair, Organizing Committee, *11th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2001)*, New York, NY, June 25-26, 2001.

JOURNAL AND CONFERENCE REFEREEING (in addition to conference program committees)

ACM Computing Surveys.

ACM Computer Communication Journal.

ACM Multimedia Conference.

ACM Multimedia Systems Journal.
ACM SIGGRAPH.
ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI).
ACM Symposium on Operating Systems Principles (SOSP).
ACM Symposium on Parallelism in Algorithms and Architectures (SPAA).
ACM Transactions on Computer Systems (TOCS).
ACM Transactions on Multimedia Computing, Communication, and Applications (TOMCCAP).
ACM Transactions on Internet Technology (TOIT).
The Computer Journal.
International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS).
IEEE GLOBECOM Technical Conference.
IEEE International Parallel and Distributed Processing Symposium (IPDPS).
IEEE Internet Computing.
IEEE Journal of Selected Areas in Communications.
IEEE Multimedia.
IEEE Transactions on Computers.
IEEE Transactions on Circuits and Systems for Video Technology.
IEEE Transactions on Mobile Computing.
IEEE Transactions on Multimedia.
IEEE Transactions on Parallel and Distributed Systems.
IEEE/ACM Transactions on Networking.
IEEE Transactions on Knowledge and Data Engineering.
IEEE Transactions on Software Engineering.
IEEE Wireless Communications and Networking Conference (WCNC).
International Conference on Dependable Systems and Networks (DSN).
International Workshop on Volume Visualization.
Journal of Parallel and Distributed Computing.
The Journal of Systems and Software.
Software Practice and Experience.
USENIX Annual Technical Conference.
USENIX Annual Technical Conference, FREENIX Track.
USENIX Conference on File and Storage Technologies (FAST).
USENIX Symposium on Networked Systems Design and Implementation (NSDI).
USENIX Security Symposium.

FUNDING AGENCIES

Participant, *NSF Cyber Trust PI Workshop*, New Haven, CT, 2008.
Participant, *NSF CISE PI Workshop*, Urbana, IL, 2005.
Participant, *NSF Cyber Trust PI Workshop*, Newport Beach, CA, 2005.
Participant, *DARPA ISAT "Law of Large Numbers System Design" Study Group*, 2005.
Grant Review Panelist, *National Science Foundation*, Arlington, VA, 2000 - 2005, 2009.

Participant, *NSF CISE PI Workshop*, Las Cruces, NM, 1999.

STANDARDIZATION COMMITTEES

Member, Net2Display Task Group, *Video Electronics Standards Association (VESA)*, 2005 - 2009.

Member, DPVL Task Group, *Video Electronics Standards Association (VESA)*, 2005 - 2006.

OUTREACH ACTIVITIES

Member, *VMAP Advisory Board*, VMware, 2009 - present.

Member, Executive Advisory Committee, *Harlem Children Society*, 2007 - present.

Mentor, Computing Innovation Fellows Project, 2009 - 2010.

Advisor, Online Membership Services Strategy, *Association for Computing Machinery*, 2007 - 2008.

Invitee, Infoscape Charrette, *Lincoln Center for the Performing Arts*, 2007.

Board Member, Membership Services Board, *Association for Computing Machinery*, 2004 - 2007.

Managing Group Member, Security and Infrastructure Standing Committee, *Financial Services Technology Consortium (FSTC)*, 2006 - 2007.

Examiner, Graduate Record Examinations (GRE) Computer Science Test, *Educational Testing Service*, 2004 - 2005.

Judge, New York City Science and Engineering Fair (NYCSEF), *New York Academy of Sciences*, 2004.

Mentor, Harlem Children Society Internship Program, *Harlem Children Society*, 2006.

Mentor, Science Research Training Program, *New York Academy of Sciences*, 2001 - 2003, 2006.

Faculty Mentor, Summer Research Program for Historically Underrepresented Groups, *Leadership Alliance*, 2000.

PROFESSIONAL SOCIETIES

Member, Association for Computing Machinery (ACM).

Senior Member, Institute of Electrical and Electronic Engineers (IEEE).

Member, New York Academy of Sciences.

Member, USENIX Association.

UNIVERSITY ACTIVITIES

(all activities at Columbia University unless otherwise noted)

DOCTORAL DISSERTATIONS SUPERVISED

1. Nicolas Viennot, Sept. 2010 - present.
2. Jeremy Andrus, Sept. 2010 - present.
3. Dan Phung, June 2004 - present.
4. Oren Laadan, Sept. 2003 - present (SEAS Presidential Fellow 2003-2007).
5. Dinesh Subhraveti, Sept. 2001 - present.
6. Alexander Sherman, "Guaranteeing Performance through Fairness in Peer-to-Peer File Sharing and Streaming Systems", Ph.D. Computer Science, defended Oct. 2009.
7. Shaya Potter, "Virtualization Mechanisms for Mobility, Security, and System Administration", Ph.D. Computer Science, May 2010, currently Postdoctoral Scholar, IBM T.J. Watson Research Center.
8. Haoqiang Zheng, "CPU Scheduling with Automatic Interactivity and Dependency Detection", Ph.D. Computer Science, defended July 2009, currently Senior Staff Engineer, VMware.
9. Ricardo Baratto, "THINC: A Virtual and Remote Display Architecture for Desktop Computing", Ph.D. Computer Science, defended Oct. 2007 (with distinction), currently Senior Software Engineer, Calista Technologies.
10. Albert M. Lai, "A Remote Training Approach for Teaching Seniors to Use a Telehealth System", Ph.D. Biomedical Informatics, Feb. 2007 (with distinction, co-advised with Justin Starren), currently Assistant Professor, Department of Biomedical Informatics, Ohio State University.
11. David P. Olshefski, "Measuring and Managing the Remote Client Perceived Response Time for Web Transactions using Server-side Techniques", Ph.D. Computer Science, Oct. 2006 (with distinction), currently Research Staff Member, IBM T.J. Watson Research Center.
12. Gong Su, "MOVE: Mobility with Persistent Network Connections", Ph.D. Computer Science, Oct. 2004, currently Research Staff Member, IBM T.J. Watson Research Center.
13. Erez Zadok, "FiST: A System for File System Code Generation", Ph.D. Computer Science, May 2001, currently Associate Professor, Department of Computer Science, Stony Brook University.

OTHER DOCTORAL DISSERTATION COMMITTEES

1. Rean Griffith, "Evaluating Software Systems via Runtime Fault-Injection and Reliability, Availability and Serviceability (RAS) Metrics and Models", Ph.D. Computer Science, Oct. 2008.
2. Stelios Sidiroglou, "Software Self-Healing Using Error Virtualization", Ph.D. Computer Science, May 2008.
3. Jacob Gorm Hansen, "Virtual Machine Mobility with Self-Migration", Ph.D. Computer Science, University of Copenhagen, Feb. 2008.
4. Hanhua Feng, "Scheduling: From Optimality to Configurability", Ph.D. Computer Science, Feb. 2008.
5. Sangho Shin, "Towards the Quality of Service for VoIP traffic in IEEE 802.11 Wireless Networks", Ph.D. Computer Science, Feb. 2008.
6. Aniruddha Bohra, "System Architectures Based on Functionality Offloading", Ph.D. Computer Science, Rutgers University, Jan. 2008.
7. Hoon Chang, "Incorporating Physical Layer Capture in the Modeling, Analysis and Design of Wireless Access Mechanisms", Ph.D. Computer Science, May 2007.
8. Xiaotao Wu, "Ubiquitous Programmable Internet Telephony End System Services", Ph.D. Computer Science, May 2007.
9. Weibin Zhao, "Towards Autonomic Computing: Service Discovery and Web Hotspot Service", Ph.D. Computer Science, May 2006.
10. Daniel Villela, "Resource Management in Large-Scale Services: Models and Algorithms", Ph.D. Electrical Engineering, Feb. 2006.

11. Yong Wang, "Resource Constrained Video Coding/Adaptation", Ph.D. Electrical Engineering, Feb. 2006.
12. Giuseppe Valetto, "Orchestrating the Dynamic Adaptation of Distributed Software with Workflow Technology", Ph.D. Computer Science, May 2004.
13. Lisa Amini, "Models and Algorithms for Resource Management in Distributed Computing Cooperatives", Ph.D. Computer Science, Feb. 2004.
14. Jonathan Lennox, "Services for Internet Telephony", Ph.D. Computer Science, Feb. 2004.
15. Raymond Liao, "Utility-Based Adaptation, Dynamic Provisioning and Incentive Engineering Techniques for Internet and its Wireless Extensions", Ph.D. Electrical Engineering, May 2003.
16. Sushil da Silva, "Netscript: A Language System for Active Networks", Ph.D. Computer Science, May 2003.
17. Maria Papadopouli, "Resource Sharing in Mobile Wireless Networks", Ph.D. Computer Science, Oct. 2002.
18. Denes Molnar, "Classical Transport Theory and Its Applications in Heavy-ion Physics", Ph.D. Physics, July 2002.
19. Apostolos Dailianas, "MarketNet: A Survivable, Market-Based Architecture for Large-Scale Information Systems", Ph.D. Computer Science, Jan. 2001.
20. Steve Dossick, "A Virtual Environment Framework for Software Engineering", Ph.D. Computer Science, Nov. 2000.

OTHER DOCTORAL EXAM COMMITTEES

1. Omer Boyaci, "Multimedia Tools for Application Sharing, Measuring Capture-to-display Latency, and User Created Services", Mar. 2010 (Thesis Proposal Committee).
2. Omer Boyaci, "Multimedia Collaboration and Application Sharing", June 2008 (Candidacy Exam Committee).
3. Stelios Sidiroglou, "Error Virtualization: A Technique for Autonomic Software Self-Healing", Dec. 2006 (Thesis Proposal Committee).
4. Hanhua Feng, "Optimal Stochastic Scheduling", Dec. 2006 (Thesis Proposal Committee).
5. Hoon Chang, "Analytical Model and Fairness Scheduling of CSMA/CA in Physical Layer Capturing", May 2006 (Thesis Proposal Committee).
6. Michael Locasto, "A Virtual CPU Framework for Self-Healing Software", Dec. 2005 (Thesis Proposal Committee).
7. Stelios Sidiroglou, "Common Mode Attacks", Nov. 2005 (Candidacy Exam Committee).
8. Rean Griffith, "Design and Implementation of Self-healing Systems", Nov. 2004 (Candidacy Exam Committee).
9. Daniel Villela, "Resource Management for Services in Federated Systems", Apr. 2004 (Thesis Proposal Committee).
10. Weibin Zhao, "Advanced Service Discovery and Web Hotspot Rescue", May 2003 (Thesis Proposal Committee).
11. Lisa Amini, "Algorithms and Protocols for Content Internetworking", Jan. 2002 (Thesis Proposal Committee).
12. Xiaotao Wu, "Telecommunication Services", Nov. 2001 (Candidacy Exam Committee).
13. Lisa Amini, "Distributed Content Services Framework", Dec. 2000 (Candidacy Exam Committee).
14. Eleazar Eskin, "Probabilistic Approaches of Anomaly Detection Applied to Intrusion Detection", May 2000 (Candidacy Exam Committee).
15. Giuseppe Valetto, "Formalisms and Mechanisms for Specifying and Supporting Coordination in Distributed Systems", Apr. 2000 (Candidacy Exam Committee).
16. Jonathan Lennox, "Advanced Services for Internet Telephony" Feb. 2000 (Thesis Proposal Committee).
17. Weibin Zhao, "Internet Quality of Service", Dec. 1999 (Candidacy Exam Committee).
18. Alexander Konstantinou, "Computational Models of Change Propagation", Dec. 1999 (Candidacy Exam Committee).
19. Ping Pan, "On Scalable Internet Resource Reservation", Apr. 1999 (Candidacy Exam Committee).

MASTERS DISSERTATIONS SUPERVISED

1. Lei Zhang, "Implementing A Windows Remote Display Architecture", M.S. Computer Science, Feb. 2006.

2. Bogdan Caprita, "Grouped Distributed Queues: Distributed Queue, Proportional Share Multiprocessor Scheduling", M.S. Computer Science, May 2005.
3. V. Guruprasad, "Canonical Simplification and Automation of the Internet", M.S. Computer Science, May 2005.
4. Wong Chun Chan, "Group Ratio Round-Robin: An O(1) Proportional Share Scheduler", M.S. Computer Science, June 2004.
5. Erik Hogstedt, "Implementing ALM: an Application-level Multicast Protocol for Group Work and Group Study", M.S. Media Technology, Royal Institute of Technology, Stockholm, Sweden, June 2002.

OTHER MASTERS DISSERTATION COMMITTEES

1. Stephen Boyd, "Practical Randomization Techniques For Combatting Code-Injection Attacks", M.S. Computer Science, May 2004.

MASTERS PROJECT STUDENTS SUPERVISED

1. Carlos Perez, M.S. Computer Science, expected May 2010 (published in *ASPLOS 2009*).
2. Jau-Yuan Chen, M.S. Computer Science, Feb. 2010.
3. Christoffer Dall, M.S. Computer Science, Feb. 2010.
4. Sinan Xiao, M.S. Computer Science, Feb. 2010.
5. Xintong Zhou, M.S. Computer Science, Feb. 2010.
6. Daniel Benamy, M.S. Computer Science, May 2009.
7. Andreas Nilsson, M.S. Computer Science, May 2009.
8. Adrian Frei, M.S. Computer Science, Feb. 2009.
9. Ke Jin, M.S. Computer Science, Feb. 2009.
10. Shariar Kazi, M.S. Computer Science, Feb. 2009.
11. Taek Joo Kim, M.S. Computer Science, Feb. 2009.
12. John Morales, M.S. Computer Science, Feb. 2009.
13. Shrinivas Nidadavolu, M.S. Computer Science, Feb. 2009.
14. Nicolas Viennot, M.S. Computer Science, Feb. 2009 (published in *ASPLOS 2009*).
15. Ken Lee, M.S. Computer Science, May 2008.
16. Divya Arora, M.S. Computer Science, Feb. 2008.
17. Jayesh Kataria, M.S. Computer Science, Feb. 2008.
18. Amortya Ray, M.S. Computer Science, Feb. 2008.
19. Dhruva Shetty, M.S. Computer Science, Feb. 2008.
20. Tarandeep Singh, M.S. Computer Science, Feb. 2008.
21. Young Jin Yoon, M.S. Computer Science, Feb. 2008.
22. Joon Seong Ahn, M.S. Computer Science, Oct. 2007.
23. Ilho Ye, M.S. Computer Science, Feb. 2007.
24. Nabahwaya Bashir-Bello, M.S. Computer Science, Feb. 2006.
25. Joeng Kim, M.S. Computer Science, Feb. 2006 (published in *WWW2006, SCC 2006*).
26. Pinxing Ye, M.S. Computer Science, Feb. 2006.
27. Sarita Bafna, M.S. Computer Science, May 2005.
28. Jonah Benton, M.S. Computer Science, May 2005.
29. Bhaygyashree Bohra, M.S. Computer Science, May 2005 (published in *WWW2004*).
30. Pavan-Kumar Josyula-Venkata, M.S. Computer Science, May 2005.

31. Leonard Kim, M.S. Computer Science, May 2005 (published in *SOSP 2005*).
32. Vijayarka Nandikonda, M.S. Computer Science, May 2005 (published in *WWW2004*).
33. Madhuri Shinde, M.S. Computer Science, May 2005.
34. Abhishek Surana, M.S. Computer Science, May 2005 (published in *WWW2004*).
35. Suchita Varshneya, M.S. Computer Science, May 2005 (published in *WWW2004*).
36. Raghu Arur, M.S. Computer Science, May 2004.
37. Paul Henley, M.S. Computer Science, May 2004.
38. Yong Gao, M.S. Computer Science, May 2003.
39. Shilpa Krishnappa, M.S. Computer Science, May 2003 (published in *WWW2003*).
40. Aparna Mohla, M.S. Computer Science, May 2003 (published in *WWW2003*).
41. Mahdi Sajjadpour, M.S. Electrical Engineering, May 2003 (published in *WWW2003*).
42. Nikhil Tiwari, M.S. Computer Science, May 2003 (published in *USENIX 2002*).
43. S. Jae Yang, M.S. Computer Science, in progress (published in *NOSSDAV 2000, PC Magazine 2001, USENIX 2001, PC Magazine 2002, USENIX 2002, TOCS 2003, WWW2003*).
44. Ravi Gadhia, M.S. Computer Science, Feb. 2003.
45. Jianqin Qu, M.S. Computer Science, May 2002.
46. Fei Li, M.S. Computer Science, Jan. 2002 (published in *DCC 2002, ICC 2002*).
47. Albert Lai, M.S. Computer Science, May 2001 (published in *SIGMETRICS 2002, TOCS 2006*).
48. Chris Vaill, M.S. Computer Science, May 2001 (published in *USENIX 2001, SIGCSE 2005, OSR 2006*).
49. Hua Zhong, M.S. Computer Science, May 2001 (published in *USENIX 2001*).
50. Rahul Joshi, M.S. Computer Science, Feb. 2001.
51. Yuan Liu, M.S. Computer Science, Oct. 2000.
52. Johan M. Andersen, M.S. Computer Science, May 2000 (published in *USENIX 2001*).
53. Sung Hyun Cho, M.S. Computer Science, May 2000.
54. Du Hee Lee, M.S. Computer Science, May 2000.
55. Naomi Novik, M.S. Computer Science, May 2000 (published in *USENIX 2001, TOCS 2003*).
56. Ari Steinfeld, M.S. Computer Science, May 2000.
57. Yue Hai Tan, M.S. Computer Science, Feb. 2000.

UNDERGRADUATE DISSERTATIONS SUPERVISED

1. Matthew Selsky, "Creating Secure Partitions for Virtualized Migration Environments", B.S. Computer Science, May 2005.

UNDERGRADUATE PROJECT STUDENTS SUPERVISED

1. David Alpert, B.S. Computer Science, May 2009.
2. Jordan Rupperecht, B.S. Computer Science, May 2009.
3. Arjun Roy, B.S. Computer Science, May 2009.
4. Andrew Shu, B.S. Computer Science, May 2009.
5. Matt Schulkind, B.S. Computer Science, May 2006.
6. Bok-Lyn Wong, B.S. Computer Science, Feb. 2006.
7. Bogdan Caprita, B.S. Computer Engineering and B.S. Applied Mathematics, Feb. 2005 (Computing Research Association's Outstanding Undergraduate Award 2004/2005 Finalist, 2005 Theodore R. Bashkow Award, published in *ANCS 2005, USENIX 2005*).

8. Yuly Finkelberg, B.S. Computer Science, May 2005.
9. Irina Likhtina, B.S. Computer Science, May 2005.
10. Robert Tobkes, B.S. Computer Science, May 2005.
11. Tony Capra, B.A. Computer Science, May 2004.
12. Dave Coulthart, B.S. Computer Science, May 2004.
13. Hubert Lin, B.S. Computer Science, May 2004.
14. Dong Lou, B.S. Computer Science, May 2004.
15. Jen Wang, B.S. Computer Science, May 2004.
16. Gerardo Flores, B.S. Computer Science, May 2003.
17. Leonard Kim, B.S. Computer Science, May 2003.
18. Sung Y. Cho, B.S. Computer Science, May 2002.
19. Erik Czernikowski, B.S. Computer Science, May 2002.
20. Aner Fust, B.S. Computer Science, May 2002.
21. Michael Kalnicki, B.S. Computer Science, May 2002.
22. Eugene Kim, B.S. Computer Science, May 2002.
23. Iliia Malkovitch, B.S. Computer Science, May 2002.
24. Steven Osman, B.S. Computer Science, May 2002 (published in *OSDI 2002*).
25. Francesco Tamburrino, B.S. Electrical Engineering, Feb. 2002.
26. Paolo de Dios, B.S. Computer Science, May 2001.
27. Carla Goldberg, B.A. Computer Science, May 2001.
28. Sara Schumacher, B.A. Computer Science, Feb. 2001.
29. Ozgur Can Leonard, B.S. Computer Science, May 2000 (published in *Dr. Dobb's Journal 2000*).

UNIVERSITY SERVICE

Member, SEAS Faculty Advisory Committee for Entrepreneurship, 2007 - present.

Faculty Advisor, Society for Entrepreneurship and Technological Innovation at Columbia University (SETI), 2008 - 2009.

Member, SEAS Nominating Committee, 2005 - 2007.

Member, Senate Committee on Athletic Eligibility, 2001 - 2008. Served on provost-appointed committee responsible for general policy on athletic eligibility and ruling on student appeals to be able to participate despite falling short of the Columbia standard for degree progress.

Member, Faculty Focus Group on Child Care, Office of Planning and Institutional Research, 2005.

Faculty Volunteer, Urban New York, Office of Student Activities, 2003 - 2007, 2010.

Member, RASCAL Project Advisory Committee, 1999 - 2001. Served on advisory committee responsible for providing guidance and feedback on the design of the electronic research administration system (RASCAL), now in use by the Office of Projects and Grants, <https://www.rascal.columbia.edu>.

Undergraduate Associate Advisor, Massachusetts Institute of Technology, 1987 - 1988.

DEPARTMENTAL SERVICE (Dept. of Computer Science unless otherwise noted)

Member and Chair, Visibility Committee, 2009 - present (Chair, 2009).

Member, Academic Committee, 2003 - 2006, 2008 - present.

USENIX Campus Liaison, USENIX Association, 2004 - present.

Faculty Organizer and Speaker, Professional Preparation Seminar Series, 2008 - 2009.

Co-Chair, Faculty Retreat, 2008.

Lab Demonstrations, Undergraduate and MS Research Project Fair, 2008.
Member and Chair, Strategic Planning Committee, 2005 - 2008 (Chair, 2007 - 2008).
Speaker, ACM Luncheon and Research Series, 2008.
Member, Faculty Recruiting Committee, 2003 - 2008.
Member and Chair, Facilities Committee, 1999 - 2006 (Chair, 2002 - 2003).
Faculty Advisor, Columbia Mainframe Computing Group, 2005 - 2006.
Member, Bill Campbell Visit Organizing Committee, 2005.
Member, Faculty Retreat Organizing Committee, 2005.
Department Representative, NSF CISE Workshop, 1999, 2005.
Member, Academic Honesty Task Force, 2004 - 2005.
Editor-in-Chief, 25th Anniversary of the Department of Computer Science Newsletter, 2004 - 2005.
Operating Systems Comprehensive Examiner, 1999 - 2004.
Speaker Host, 25th Anniversary Distinguished Lecture Series, 2004.
Lab Demonstrations, 25th Anniversary of the Department of Computer Science, 2004.
Speaker, 25th Anniversary of the Department of Computer Science, 2004.
Columbia College Academic Advisor (Seniors), 2003 - 2004.
Lab Demonstrations, ACM Computer Science Research Fair, 2003.
Ph.D. Funding Survey, Ph.D. Committee, 2003.
Chair, CRF Director Search Committee, 2003.
Columbia College Academic Advisor (Juniors), 2002 - 2003.
Departmental Infrastructure and Systems Area Speaker, External Review, 2003.
Research Demonstration, CAP Computer Science Research Fair, 2002.
Speaker, ACM Computer Science Research Fair, 2002.
Speaker, Faculty Research Colloquia, 2002.
Faculty Assistant Manager, 2000 - 2002.
Columbia College Academic Advisor (Freshman and Sophomores), 2001 - 2002.
Member, Ph.D. Admissions Committee, 1999 - 2002.
Speaker, ACM Computer Science Research Fair, 2001.
Speaker, Faculty Research Colloquia, 2001.
M.S. Academic Advisor, 1999 - 2001.
Department Faculty Representative, SEAS Engineering Council, 2001.
Speaker, ACM Computer Science Research Fair, 2000.
SEAS New Graduate Student Orientation, 2000.
Computer Science Colloquium Chair, 1999 - 2000. Faculty comments: "This seems to have been the most interesting set of colloquia since I've been at Columbia." (Feb. 2000). "I keep having to change plans because you've organized such a terrific colloquium series." (Feb. 2000). "Just fyi, that was one of the best colloquia I've ever been to in my life!" (Dec. 1999).
SEAS Alumni Faculty-Student Dinners, 1999.
Graduate Admissions Committee, Dept. of Electrical Engineering, Stanford University, 1996.
Graduate Mentor, Dept. of Electrical Engineering, Stanford University, 1993 - 1995.

CURRICULUM AND TEACHING

(all activities at Columbia University unless otherwise noted)

NEW CURRICULUM DEVELOPMENT

COMS E6998 Mobile Computing with iPhone and Android, 2008 - present. Developed and taught a new course on smartphone mobile computing that explores the technologies and convergence of computing, telephony, and sensors in the physical world. Course has also been profiled in:

Elizabeth Woyke, "iPhone and Android Apps 101", *Forbes.com*, New York, NY, Nov. 2008.

COMS E6998 Virtual Machines, 2007 - 2008. Co-developed and taught a new advanced graduate course on virtual machines.

COMS E6998 Topics in Computer Systems, 2005 - 2006. Developed and taught a new advanced graduate course on topics in computer systems which focuses on a different technical area of interest each semester.

COMS W4118 Operating Systems, 1999 - 2004. Developed and taught a new advanced undergraduate / graduate course in operating systems, which integrates operating system concepts with real-world operating system design and implementation. First course in the world to employ novel virtual machine technology to provide hands-on operating system design and implementation instruction in a real commercial operating system for both on-campus and distance learning students. Approach has been emulated at several other universities, including Calvin College, Clarkson University, John Hopkins University, SUNY Stony Brook, Swarthmore College, University of Illinois, University of Rochester, University of Virginia, University of Washington, Worcester Polytechnic Institute, etc. "The best CS class of my college career, both in terms of how much I learned and how valuable the information turned out to be in the real world. Writing new system calls, device drivers, schedulers... Mention to an interviewer that you know how to do this and they drool..." *Slashdot*, Dec. 2000. Course has also been profiled in:

"Software Doubles as Insurance Policy for Columbia University", *College Planning and Management*, Apr. 2001.

Charles Babcock, "VMware Welcomes Guest OSes", *Inter@ctive Week*, 7(17), Ziff-Davis Media, New York, NY, May 1, 2000, p. 86.

Mara Velasco Sweet, "Columbia Students Gain Valuable Experience in Operating System Design Using VMware", *VMware Customer Success Stories*, VMware, Palo Alto, CA, Oct. 1999.

COMS E6118 Advanced Operating Systems, 2000 - 2004. Developed and taught a new advanced graduate course in operating systems. New classroom and lab course materials were developed on recent research developments in operating systems. Course also develops research skills by emphasizing classroom discussion, student presentation skills, and in-depth programming projects.

COMS W3157 Advanced Programming, 2001. Helped formulate and develop an undergraduate advanced programming course with an emphasis on systems programming principles and tools.

COMS W3139 Data Structures and Algorithms in Java, 1999. Developed and taught a new undergraduate course in data structures and algorithms using Java. Previous versions of the course were taught in C, but a department decision to move the core undergraduate computer science curriculum to Java created a critical need for this course. New Java-based course materials were developed and have been subsequently been used by other faculty for this course.

TEACHING EXPERIENCE

COMS W3998 Projects in Computer Science, Fall 2000 - present. Enrollment 2 (Fall 2000), 1 (Spring 2001), 1 (Fall 2001), 2 (Spring 2002), 1 (Fall 2002), 2 (Spring 2003), 2 (Fall 2003), 3 (Spring 2004), 2 (Fall 2004), 1 (Fall 2005).

COMS W4901 Projects in Computer Science, Summer 1999 - present. Enrollment 1 (Summer 1999), 3 (Spring 2000), 2 (Summer 2000), 3 (Spring 2001), 1 (Fall 2001), 2 (Spring 2002), 3 (Spring 2003), 2 (Fall 2003), 2 (Fall 2005), 1 (Fall 2006), 4 (Fall 2008), 3 (Spring 2009).

COMS E6901 Projects in Computer Science, Spring 1999 - present. Enrollment 1 (Spring 1999), 8 (Fall 1999), 7 (Spring 2000), 2 (Summer 2000), 4 (Fall 2000), 4 (Spring 2001), 6 (Fall 2001), 6 (Spring 2002), 10 (Fall 2002), 5 (Spring 2003), 11 (Fall 2003), 2 (Spring 2004), 6 (Fall 2004), 6 (Spring 2005), 1 (Fall 2005), 3 (Spring 2006), 7 (Fall 2006), 2 (Spring 2007), 2 (Fall 2007), 6 (Spring 2008), 5 (Fall 2008) 4 (Spring 2009), 1 (Summer 2009), 1 (Fall 2009), 2 (Spring 2010).

COMS E6118 Advanced Operating Systems, Spring 2010. Enrollment 5 (2 CVN).

COMS W4118 Operating Systems, Fall 2009. Enrollment 65 (7 CVN), instructor rating 4.1/5.0.

COMS E6998 Mobile Computing with iPhone and Android, Summer 2009. Enrollment 4 (CVN pre-taped).

COMS W4118 Operating Systems, Summer 2009. Enrollment 8 (CVN pre-taped).

COMS E6998 Mobile Computing with iPhone and Android, Spring 2009. Enrollment 70 (14 CVN), instructor rating 3.9/5.0.

COMS W4118 Operating Systems, Fall 2008. Enrollment 74 (13 CVN), instructor rating 4.5/5.0.

COMS E6998 Virtual Machines, Spring 2008. Enrollment 24 (6 CVN), instructor rating 4.8/5.0.

COMS W4118 Operating Systems, Fall 2007. Enrollment 42, instructor rating 4.1/5.0.

COMS E6998 Topics in Computer Systems, Spring 2006. Enrollment 7, instructor rating 5.0/5.0.

COMS E6118 Advanced Operating Systems, Fall 2005. Enrollment 13, instructor rating 4.4/5.0.

COMS W4118 Operating Systems, Fall 2004. Enrollment 100 (16 CVN), instructor rating 4.3/5.0.

COMS W4118 Operating Systems, Summer 2004. Enrollment 4 (CVN pre-taped).

COMS E6118 Advanced Operating Systems, Spring 2004. Enrollment 22, instructor rating 4.3/5.0.

COMS W4118 Operating Systems, Fall 2003. Enrollment 83 (10 CVN), instructor rating 4.2/5.0.

COMS W4118 Operating Systems, Summer 2003. Enrollment 2 (CVN pre-taped).

COMS W4118 Operating Systems, Spring 2003. Enrollment 75 (5 CVN), instructor rating 4.2/5.0.

G22.3813 Advanced Laboratory in Computer Science, New York University, Spring 2003. Enrollment 1.

COMS W4118 Operating Systems, Fall 2002. Enrollment 84 (14 CVN), instructor rating 4.2/5.0.

COMS W4118 Operating Systems, Summer 2002. Enrollment 7 (CVN pre-taped).

COMS E6118 Advanced Operating Systems, Spring 2002. Enrollment 17, instructor rating 4.4/5.0.

COMS W4118 Operating Systems, Spring 2002. Enrollment 6 (CVN pre-taped).

COMS W4118 Operating Systems, Fall 2001. Enrollment 102 (16 CVN), instructor rating 4.1/5.0.

COMS W4118 Operating Systems, Summer 2001. Enrollment 8 (CVN pre-taped).

COMS E6118 Advanced Operating Systems, Spring 2001. Enrollment 5, instructor rating 4.4/5.0.

COMS W4118 Operating Systems, Fall 2000. Enrollment 127 (19 CVN), instructor rating 3.8/5.0.

COMS E6118 Advanced Operating Systems, Spring 2000. Enrollment 23, instructor rating 3.9/5.0.

COMS W4118 Operating Systems, Fall 1999. Enrollment 119 (11 CVN), instructor rating 3.8/5.0.

COMS E6901 Operating Systems and Networking Reading Seminar, Fall 1999.

COMS W3139 Data Structures and Algorithms in Java, Spring 1999. Enrollment 52, instructor rating 4.2/5.0. (nominated for Columbia Great Teacher Award)

Intermediate Guitar, Christian Guitarist Conference, Apr. 1996, 1997, 1998.

SELECTED STUDENT COURSE EVALUATION COMMENTS

“Great teaching and organization, the best CS course.” (Fall 2009)

“I got to learn the most out of any course in my 2 years at Columbia.” (Fall 2009)

“A true master of the subject matter; excellent classroom delivery; and unafraid to innovate around the homework assignments (Android, Git, VMs, etc).” (Fall 2009)

“I had Jason Nieh for both Operating Systems and this course. He is a great lecturer that really knows how to motivate students to learn.” (Spring 2009)

"I love the concept of the class and I believe it's vital for students to continue broadening their skill sets to encompass more than just your usual CS topics. There was a lot of self-exploration but I felt that Professor Nieh did an excellent job keeping everyone engaged for the entire semester. That surely isn't easy." (Spring 2009)

"I'm so glad I took this course. It was so much fun...amazing course." (Spring 2009)

"Professor Nieh is the best professor I've studied under at Columbia University. His high standards boundless energy and ability to draw students into the lecture are amazing. His class is known for being the toughest and most demanding in our program. Yet I looked forward each day to attending his lectures and attacked the difficult problem sets with motivation and vigor unlike any other class. He inspires students to do the tough work not unlike the manner in which an athletic coach pushes and motivates his or her players. I wanted to do well in this class wanted to pull the countless all nighters if for no other reason than having the pride and incredible sense of accomplishment that comes with being able to hang with Jason Nieh. We need more professors like this who are able to set incredibly high standards while also inspiring students to achieve them while at the same time leaving the student with a very solid understanding of theory and very marketable skills." (Fall 2008)

"This course is the best CS course I have ever taken...Jason is an excellent teacher, who is very approachable and answers any question with insight and dedication, so take this course with him if you have the chance." (Fall 2008)

"This is by far the most demanding and rewarding class I have taken as a CS grad student at Columbia." (Fall 2008)

"Prof. Nieh is amazingly knowledgeable in this area and is able to communicate the material in an effective interesting manner that truly captivates students attention. Undoubtedly the best CS lecturer I have come across at Columbia." (Fall 2008)

"The best instructor I've encountered at CU." (Fall 2008)

"OS is the most thorough classes I've taken and has taught me the most." (Fall 2008)

"Prof. Nieh really knows his stuff and has some pretty amazing homework lined up. You can tell he put a lot of work into designing problems that seem plausible and teach you a lot. Much to my classmates chagrin I'd say the homework is the best part of the class." (Fall 2008)

"...the best course I have taken. So much to learn and the hands-on Linux kernel development is fantastic." (Fall 2008)

"Professor is amazing." (Fall 2008)

"Great course. I actually look forward to going to class each lecture. The instructor is very engaging -- by far the best lecturer I've had at CU...The class is tough but I really feel like I am getting a ton of value out of it." (Fall 2008)

"The professor and TAs definitely know the material inside-out and the lectures are excellent and far more educational than other classes I've taken in the CS dept." (Fall 2008)

"...I really enjoyed OS...(undoubtedly) the most challenging course I've taken, but it was the most interesting and I believe will be the most useful." (Fall 2008)

"One of the best courses taken..." (Spring 2008)

"This class was the class I have learned the most from, and has also been the class from which I have gained the most marketable skills I have and have at least indirectly landed me job offers." (Fall 2007)

"I probably learned more in this course than my last three CS courses combined." (Fall 2007)

"Prof. Nieh is the greatest teacher I ever met." (Fall 2004)

"Best CS teacher at Columbia hands down." (Fall 2004)

"The best lecturer I have ever." (Fall 2004)

"The best one (course) I have ever taken..." (Fall 2004)

"Amazing class and teacher." (Fall 2004)

"Brilliant, knowledgeable, approachable professor." (Fall 2004)

"There's nothing he can't do." (Fall 2004)

"Outstanding professor. Knows EVERYTHING about linux and operating systems in general." (Fall 2004)

"...definitely recommended for any Computer Science student." (Fall 2004)

“Dr. Nieh took a potentially dry topic and made it very interesting. The classroom was very crowded throughout the semester: not just because there were way too many desks and not enough space, but because Dr. Nieh made lectures intriguing enough that most students always came.” (Fall 2004)

“Dr. Nieh is a great professor. I took an Operating Systems course at my undergrad university, and it was very dry. Dr. Nieh made the lectures interesting, and he kept our attention...” (Fall 2004)

“One of the best! If we had more professors like this one, the MS would be number 1!” (Fall 2004)

“I rate this one of the best courses in Columbia University.” (Fall 2004)

“...a fun and highly informative class!” (Fall 2004)

“...my favorite. Being able to hack the Linux kernel is awesome. I am learning a lot. And Professor Nieh’s delivery is second to none...I really do love the course.” (Fall 2004)

“...extremely well organized and handled, despite having a huge number of students.” (Fall 2004)

“Best teacher I have had so far.” (Fall 2003)

“Great teacher, great course. Extremely clear about why things are how they are. Challenges the students to think through the answer instead of just stating it, which too few professors in CS do.” (Fall 2003)

“...a master in his field...a brilliant orator, presenter and well a learned man all in one.” (Fall 2003)

“Professor Nieh runs a class that is orders of magnitude more organized and more thoughtfully planned. He’s structured unbelievably dense material extremely well so that I’m able to follow the course of the subject easily.” (Fall 2003)

“The course material was invaluable. The skills and knowledge you learn are immense.” (Fall 2003)

“...the most enjoyable, informative, and well-structured course...every CS student at Columbia should not miss out the opportunity to learn under him.” (Fall 2003)

“Best lecturer in Computer Science in my academic career.” (Fall 2003)

“The best CS class I’ve had, combines very well theory and practice.” (Fall 2003)

“I recommend more in-depth classes on operating systems to be taught by Prof. Nieh.” (Fall 2003)

“Professor Nieh clearly knows his stuff about OS and is able to teach it to his students very well.” (Fall 2003)

“Very organized, approachable, unlike some professors, knows his stuff very very well. Overall, an awesome professor.” (Fall 2003)

“Professor Nieh is very approachable and extremely knowledgeable. He exudes everything that a teacher should be.” (Fall 2003)

“Knows the subject inside out...very approachable and friendly...strives to provide a quality class, makes no compromises.” (Fall 2003)

“...knows his subject so well...amongst the best professors I have met.” (Fall 2003)

“...very well-lectured and well-run, and I was impressed by the amount that we learned.” (Fall 2003)

“...a very good professor who knows how to relate a difficult subject in a very easy to understand manner.” (Fall 2003)

“Great teacher...you’ll get a lot out from this class, in terms of programming skills and systems knowledge in general...definitely one of the best CS classes I took at Columbia.” (Spring 2003)

“Nieh is an awesome teacher that is very organized and that instructs his class with a lot of thought behind everything.” (Spring 2003)

“Nieh is clear, concise, and eminently knowledgeable within the contemporary operating systems field.” (Spring 2003)

“The best CS professor I have taken a class with.” (Spring 2003)

“Prof. Nieh is very friendly, very knowledgeable in his field and very open to students.” (Spring 2003)

“A tremendous amount of thought was clearly put into the course design. One of the best organized classes I’ve been in.” (Spring 2003)

“Professor Nieh is a great and very knowledgeable professor. He is also always available and willing to help.” (Spring 2003)

“Best organized class I’ve taken so far. Professor Nieh really cares about what people learn, and he takes his job seriously.” (Spring 2003)

“I’m really impressed...never had a course like this...” (Spring 2003)

“Prof. Nieh is an excellent teacher. He is always prepared for class. He maintains an outstanding course website. He also addresses student questions and allows them to think in the classroom... he is very approachable and is a really nice guy...you also gain a lot from the class.” (Spring 2003)

“Nieh is a terrific instructor. He has a gift for selecting just the right details to demonstrate a particular point so that the rest of the material falls into place...” (Fall 2002)

“I have not come across a professor as good as he is in my life.” (Fall 2002)

“Professor Nieh takes what is possibly the most difficult topic in Computer Science and explains it in a way that makes difficult topics seem almost common-sense. His classroom delivery is impeccable, and the amount learned is incredible.” (Fall 2002)

“Nieh is gifted; he has an ability to communicate ideas both colloquially but also with appropriate technical precision.” (Fall 2002)

“Aside from knowing his stuff, Prof. Nieh has a great style of lecturing. He always comes prepared, always ready to answer questions, and actually gets you to think about the material.” (Fall 2002)

“Great professor, knows his stuff.” (Fall 2002)

“Nieh is one of the best professors in the CS department...was always available whether during office hours or not. Compared to other professors, he is a much better speaker and has better presentation skills. His knowledge of subject matter is on par with other great professors I’ve had. Most importantly, he’s a nice and understanding guy which is very welcome in a department of professors who seem like they’re out to get you. I learned a tremendous amount and thoroughly enjoyed the class.” (Fall 2002)

“A very good instructor in all the sense of the word. He knows his material, listens to students, and is willing to help the students.” (Fall 2002)

“...made the Linux kernel accessible to students to a degree I wouldn’t have imagined possible.” (Fall 2002)

“It’s a great, great class.” (Fall 2002)

“Very, very knowledgeable and easily approachable.” (Fall 2002)

“Highly recommended...” (Spring 2002)

“This class was fun. It’s laid back and very instructive...” (Spring 2002)

“This is an excellent class.” (Spring 2002)

“Prof. Nieh is by far the best professor I have encountered in this school.” (Fall 2001)

“Must-take class for all CS majors.” (Fall 2001)

“The best CS class of my college career, both in terms of how much I learned and how valuable the information turned out to be in the real world. Writing new system calls, device drivers, schedulers... Mention to an interviewer that you know how to do this and they drool...” (Fall 2000)

“Hardest, but best class I’ve taken so far at Columbia...” (Fall 2000)

“This is the best course I have taken in 6 years at the CS dept.” (Spring 2000)

“I love that we’re working with a real OS like Linux. Doing the homework was fun, particularly so because it felt like really accomplishing something of practical value.” (Fall 1999)

“A relative new-comer to Columbia, Nieh is a VERY smart guy, and when it comes to OS, he is THE specialist. His lectures are one of the better ones here at Columbia, and you’ll actually learn a lot.” (Fall 1999)

“A great course, I really enjoyed it. Thanks.” (Spring 1999)

“Best course I’ve taken at Columbia thus far.” (Spring 1999)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
 Edmund Munger, et al.)
)
 U.S. Patent No.: 7,188,180)
 Filed: November 7, 2003) Examiner:
 Issued: March 6, 2007) Andrew L. Nalven
)
 For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
 SECURE COMMUNICATION LINK)
 BETWEEN COMPUTERS OF)
 VIRTUAL PRIVATE NETWORK)
)
 Reexamination Proceeding)
 Control No.: 95/001,270)
 Filed: December 8, 2009)

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132, filed with United States Patent and Trademark Office on April 19, 2010, was served this 19th day of April, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Patent Owner
**Please recognize our Customer No. 23630 as
our correspondence address.**

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: April 19, 2010

Electronic Acknowledgement Receipt

EFS ID:	7444671
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	19-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:40:05
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Nieh_Declaration.pdf	1488660 <small>39f74042d0fcc15599d3b66aa6721cf03e5a0ec8</small>	no	45

Warnings:

Information:

2	Reexam Certificate of Service	Cert_Serv_Nieh.pdf	24155 2834a429e9606e2234d7163c061a5f3be2978427	no	1
---	-------------------------------	--------------------	---------------------------------------------------	----	---

Warnings:

Information:

Total Files Size (in bytes):	1512815
-------------------------------------	---------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Patent Application Fee Transmittal

Application Number:	95001270
Filing Date:	08-Dec-2009
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	077580-0090

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Petition fee- 37 CFR 1.17(f) (Group I)	1462	1	400	400

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				400

Electronic Acknowledgement Receipt

EFS ID:	7444741
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	19-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:51:06
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$400
RAM confirmation Number	6364
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	Petition for review/processing depending on status	Petition_Suspend.pdf	141569 b504d1bbfcc1e1d8af3e56ca39a3cc7350937fd9	no	16

Warnings:

Information:

2	Reexam Certificate of Service	Cert_Serv_Suspend.pdf	27518 0caf698a84a246512801644df33830c4e27b66c5	no	1
---	-------------------------------	-----------------------	---------------------------------------------------	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	30500 b13fc6011fed3ce63e616f7a44dfed6bb38242	no	2
---	-------------------------	--------------	-------------------------------------------------	----	---

Warnings:

Information:

Total Files Size (in bytes):

199587

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Patent Application Fee Transmittal

Application Number:	95001270
Filing Date:	08-Dec-2009
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Filer:	William Neal Hughet/Tamika Miles
Attorney Docket Number:	077580-0090

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Petition fee- 37 CFR 1.17(f) (Group I)	1462	1	400	400

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				400

Electronic Acknowledgement Receipt

EFS ID:	7540831
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	William Neal Hughet/Tamika Miles
Filer Authorized By:	William Neal Hughet
Attorney Docket Number:	077580-0090
Receipt Date:	03-MAY-2010
Filing Date:	08-DEC-2009
Time Stamp:	18:33:01
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$400
RAM confirmation Number	11350
Deposit Account	022135
Authorized User	

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		PetitionPursuantTo37CFR183.pdf	766966 36bc935c93344d96e5c1f0cb646ca5f190d9927f	yes	14

Multipart Description/PDF files in .zip description

Document Description	Start	End
Reexam - Opposition filed in response to petition	1	13
Reexam Certificate of Service	14	14

Warnings:

Information:

2	Fee Worksheet (PTO-875)	fee-info.pdf	30504 104e5bd94b1c82130a8b875ed0525e4740439015	no	2
---	-------------------------	--------------	---------------------------------------------------	----	---

Warnings:

Information:

Total Files Size (in bytes): 797470

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,270	12/08/2009	7188180	077580-0090	2128

23630 7590 05/12/2010

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

EXAMINER

ART UNIT PAPER NUMBER

DATE MAILED: 05/12/2010

Please find below and/or attached an Office communication concerning this application or proceeding.



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

MAY 12 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)



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

Toby H. Kusmer
McDermott Will & Emery
600 13th Street, NW
Washington DC 20005-3096

(For Patent Owner)

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street NW
Suite 800
Washington, D.C 20005

(For *Inter Partes* Requester)

MAILED

MAY 12 2010

CENTRAL REEXAMINATION UNIT

In re Larson et al.
Inter partes Reexamination Proceeding
Control No. 95/001,270
Filed: December 8, 2009
For: U.S. Patent No. 7,188,180

: **DECISION**
: **DISMISSING**
: **PETITIONS**
:

This is a decision on the April 19, 2010 patent owner Petition To Suspend *Inter Partes* Reexamination Proceedings Pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. §§ 1.181, 1.182, 1.183, and 1.987 and on the April 19, 2010 patent owner Petition Pursuant to 37 C.F.R. § 1.182 for OPLA to Take and Retain Jurisdiction Over These *Inter Partes* Reexamination Proceedings. The patent owner petition to suspend is taken as a petition under 37 C.F.R. § 1.182, because the rules do not provide for the filing of a petition requesting that an *inter partes* reexamination proceeding be suspended.

This is also a decision on the May 3, 2010 Third Party Requester's Petition Pursuant to 37 C.F.R. § 1.183 and/or 1.182 in Opposition to Patent Owner's Petition to Suspend *Inter Partes* Reexamination Proceedings. The petition is taken under 37 C.F.R. § 1.182, because the rules do not provide for the filing of an opposition petition

The petition fee of \$400.00 pursuant to 37 C.F.R. § 1.17(f) for each of patent owner's petitions under 37 C.F.R. § 1.182 was charged to patent owner's deposit account 501133, as authorized by the patent owner.

The petition fee of \$400.00 pursuant to 37 C.F.R. § 1.17(f) for third party requester's petition was charged to third party requester's deposit account 022135, as authorized by the third party requester.

The proceeding, patent owner petitions, and third party requester petition are before the Office of Patent Legal Administration for consideration.

SUMMARY

1. The patent owner petition under 37 C.F.R. §§ 1.181, 1.182, 1.183 and 1.987 and 35 U.S.C. § 314(c) is dismissed.
2. The patent owner petition under 37 C.F.R. § 1.182 for OPLA to take and retain jurisdiction is granted to the extent that OPLA has taken jurisdiction to decide patent owner's petitions, and dismissed as to the request that OPLA retain jurisdiction, since such would run contrary to the mandate of 35 U.S.C. 314 (c) for special dispatch in reexamination proceedings.
3. The third party requester's petition pursuant to 37 C.F.R. § 1.183 and/or § 1.182 in opposition to patent owner's petition is granted to the extent that the petition has been entered and considered.

REVIEW OF FACTS

1. U.S. Patent No. 7,188,180 (the '180 patent) issued to Larson et al. on March 6, 2007, with 41 claims.
2. A civil litigation involving the '180 patent, captioned *VirnetX, Inc. v. Microsoft Corporation*, U.S. District Court, Texas Eastern, Case No. 6:07cv80, is pending.
3. On November 25, 2009, a request for *inter partes* reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent was deposited by a third party requester, Microsoft Corporation (a party to the concurrent civil litigation). A corrected request was filed December 8, 2009, which received a filing date and was assigned control no. 95/001,270 (the '1270 proceeding).
4. On January 19, 2010, reexamination was ordered for claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent.
5. On January 19, 2010, a first Office action was issued rejecting claims 1, 10, 12-15, 17, 26, 28-31, and 33 and confirming claims 4, 20, and 25. The remaining claims are not subject to reexamination.
6. On February 22, 2010, patent owner petitioned for an extension of time, which was granted in part on February 25, 2010, extending the period for response to April 19, 2010.
7. On March 25, 2010, patent owner filed a notice of concurrent proceedings, including a March 16, 2010 jury verdict in the concurrent litigation finding claims 1, 4, 15, 17, 20, 31, 33, and 35 willfully infringed and not invalid, and a notice that a new complaint was filed on March 17, 2010 against Microsoft based on infringement of the '180 patent in the Eastern District of Texas, Case No. 6:10cv94.

8. On April 19, 2010, patent owner filed a response to the January 19, 2010, non-final action.
9. On April 19, 2010, patent owner also filed the subject petitions requesting that this proceeding be suspended and that OPLA take and retain jurisdiction over the '1270 proceeding.
10. On May 3, 2010 third party requester filed the subject petition in opposition to patent owner's petition for suspension.

DECISION

I. RELEVANT STATUTES, REGULATIONS, AND EXAMINING PROCEDURE

35 U.S.C. 314 (c) states:

SPECIAL DISPATCH.- Unless otherwise provided by the Director for good cause, all inter partes reexamination proceedings under this section, including any appeal to the Board of Patent Appeals and Interferences, shall be conducted with special dispatch within the Office.

35 U.S.C. 317(b) states:

FINAL DECISION.- Once a final decision has been entered against a party in a civil action arising in whole or in part under section 1338 of title 28, that the party has not sustained its burden of proving the invalidity of any patent claim in suit or if a final decision in an inter partes reexamination proceeding instituted by a third-party requester is favorable to the patentability of any original or proposed amended or new claim of the patent, then neither that party nor its privies may thereafter request an inter partes reexamination of any such patent claim on the basis of issues which that party or its privies raised or could have raised in such civil action or inter partes reexamination proceeding, and an inter partes reexamination requested by that party or its privies on the basis of such issues may not thereafter be maintained by the Office, notwithstanding any other provision of this chapter. This subsection does not prevent the assertion of invalidity based on newly discovered prior art unavailable to the third-party requester and the Patent and Trademark Office at the time of the inter partes reexamination proceedings.

37 C.F.R. § 1.182 states (in part):

All situations not specifically provided for in the regulations of this part will be decided in accordance with the merits of each situation by or under the authority of the Director, subject to such other requirements as may be imposed, and such decision will be communicated to the interested parties in writing. Any petition seeking a decision under this section must be accompanied by the petition fee set forth in § 1.17(f).

37 C.F.R. § 1.907 states (in part):

(b) Once a final decision has been entered against a party in a civil action arising in whole or in part under 28 U.S.C. 1338 that the party has not sustained its burden of proving invalidity of any patent claim-in-suit, then neither that party nor its privies may thereafter request *inter partes* reexamination of any such patent claim on the basis of issues which that party, or its privies, raised or could have raised in such civil action, and an *inter partes* reexamination requested by that party, or its privies, on the basis of such issues may not thereafter be maintained by the Office.

37 C.F.R. § 1.987 states:

If a patent in the process of *inter partes* reexamination is or becomes involved in litigation, the Director shall determine whether or not to suspend the *inter partes* reexamination proceeding.

The Manual of Patent Examining Procedure (MPEP) § 2686.04, subsection V, states (in part):

* * * * *

The statute thus authorizes the Director of the USPTO to suspend (stay) reexamination proceedings, where there is good cause to do so, pending the conclusion of litigation based on a potential for termination of a reexamination prosecution under 35 U.S.C. 317(b). Thus, a District Court decision that is pending appeal on the validity of the same claims considered in an *inter partes* reexamination proceeding may provide the requisite statutory "good cause" for suspension, due to the real possibility that the 35 U.S.C. 317(b) estoppel may attach in the near future to bar/terminate the reexamination proceeding. Any such fact situation is resolved on a case-by-case basis.

In any *inter partes* reexamination where the requester (or its privies) is also a party to ongoing or concluded litigation as to the patent for which reexamination has been requested, the potential for this statutory estoppel to attach must be considered.

* * * * *

Taking the above into account, the following factors are to be considered in determining whether it is appropriate to refuse to order an *inter partes* reexamination, terminate the reexamination, or suspend action in the reexamination, based on litigation in which the reexamination requester is a party to the litigation.

(A) The 35 U.S.C. 317(b) estoppel applies only to patent claims that were litigated in the suit, i.e., litigated claims. The estoppel does not apply to non-litigated patent claims. Where there are non-litigated claims for which reexamination had been requested in the *inter partes* reexamination request, the reexamination proceeding is to go forward based on those non-litigated claims. If, however, during the reexamination proceeding, the patent owner disclaimed all the non-litigated claims, leaving only litigated claims, the proceeding is to be referred to the Office of Patent Legal Administration (OPLA).

(B) The 35 U.S.C. 317(b) estoppel applies only to issues which the requester or its privies raised or could have raised in the civil action. The estoppel does not apply where new issues are raised in the request. If the request provides new art/issues not raised in the litigation (civil action), and which could not have been so raised, then estoppel does not attach. The patent owner has the burden of showing that the art and issues applied in the request was available to the third-party requester and could have been placed in the litigation.

(C) The 35 U.S.C. 317(b) estoppel applies only in a situation where a final decision adverse to the requester has already been issued. If there remains any time for an appeal, or a request for reconsideration, from a court (e.g., District Court or Federal Circuit) decision, or such action has already been taken, then the decision is not final, and the estoppel does not attach. A stay/suspension of action may be appropriate for the reexamination proceeding if the litigation has advanced to a late enough stage and there is sufficient probability that a final decision will be adverse to the requester; however, that is a matter to be discussed with the OPLA in any such instance.

(D) Is there a concurrent *ex parte* reexamination proceeding for the patent?

II. DISCUSSION

A. Patent Owner Requests Suspension of the '1270 Proceeding

Petitioner asserts that good cause exists to suspend the '1270 proceeding because a jury verdict has been issued in the district court proceeding. Petitioner argues that when the jury verdict

becomes final, the third party requester will be estopped from further addressing the present rejections in the '1270 proceeding because the grounds of rejection of claims 1, 4, 15, 17, 20, 31, 33, and 35 were raised by the third party requester in the litigation.

Petitioner asserts that the facts of this proceeding closely follow the facts of *In re Tremblay et al.*, Reexamination Control No. 95/000093, (*Sony*)¹ in which the proceeding was suspended, except that in this proceeding, the third party requester initiated proceedings three and one-half months prior to the jury verdict rather than shortly after the verdict in *Tremblay*. There are far more significant differences between this proceeding and *Tremblay* than the timing of the filing of the request for reexamination. Most importantly, the concurrent litigation in *Tremblay* was at the appellate stage and the appeal had been briefed at the U.S. Court of Appeals for the Federal Circuit (hereinafter, the "Federal Circuit"). In the present proceeding, briefing and post-trial motions at the district court have not even concluded. The time for seeking appeal has not begun to run. The concurrent litigation is not final, nor is it close to being final. As acknowledged by petitioner on page 6 of the petition, opening motions have begun, replies are not due until May, and the hearing has been rescheduled for May 27.² After the hearing, if a final judgment is entered by the district court, Microsoft will have the opportunity to file an appeal, which will then require briefing and will be heard on a normal schedule.

As claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 have already been subject to an Office action and a response has been filed in this reexamination proceeding, the examiner is ready to take further action now. It is likely that the reexamination proceeding will be completed well before the concurrent litigation becomes final after appeal is exhausted.

B. Patent Owner Requests for OPLA to Take and Retain Jurisdiction of the '1270 Proceeding

Patent owner petitions for OPLA to take jurisdiction of the '1270 proceeding to decide the petition to suspend, to decide and issue a decision on the petition to suspend, and to retain jurisdiction until 30 days following a decision. OPLA has taken jurisdiction and has decided the petition for suspension; however, there is no reason for OPLA to retain jurisdiction after this decision. To the contrary, retaining jurisdiction would retard the statutorily mandated special dispatch required (see 35 U.S.C. 314(c)) in resolving the substantial new questions of patentability raised by the reexamination request.

C. Third Party Requester's Petition in Opposition to Patent Owner's Request for Suspension

Third party requester petitions to submit arguments in opposition to the patent owner's request for suspension of the proceeding. The petition is entered to the extent that the arguments have been considered. The patent owner's request for suspension is decided and explained below in section D.

¹ See, the related litigation titled *Sony Computer Entertainment America Inc. v. Dudas*, 2006 U.S. Dist. LEXIS 36856, (E.D.VA 2006).

² According to the facts recited in third party requester's opposition petition, the hearing has been rescheduled for June 2, 2010.

D. Additional Analysis and Findings

The factors to be considered in determining whether it is appropriate to terminate action in an *inter partes* proceeding based on a concluded litigation in which the third party requester is a party to the litigation are detailed in MPEP 2686.04, subsection V, reproduced above. In this case, the civil litigation and the '1270 proceeding both involve the claims 1, 4, 15, 17, 20, 31, 33, and 35 of the '180 patent, with the '1270 proceeding additionally conducting reexamination of dependent claims 10, 12-14, 26, and 28-30. The patent owner has raised the presumption that the prior art issues in the '1270 proceeding are the same issues that are raised or could have been raised in the civil litigation. This presumption has not been rebutted by the third party requester. There is no concurrent *ex parte* proceeding for the '180 patent.

The above factors indicate that estoppel may, in the future, attach to claims 1, 4, 15, 17, 20, 31, 33, and 35 in the *inter partes* proceeding; however, the most significant factor is whether a final decision adverse to the requester has been issued. In this case, no final decision has been issued. Even where a decision has not yet become final, a *stay or suspension* of a proceeding may be appropriate if (a) all other factors for estoppel attachment are present and (b) the litigation has advanced to a late enough stage that a final decision will be rendered in the near future and there is sufficient probability that a final decision will be adverse to the requester based solely on the prior district court decision (the Office cannot enter into the appeals court's province to try to assess the probability as to which party will win on appeal). In this situation, the district court judgment has not been made final, and the opportunity to appeal to the Federal Circuit has not commenced.

Thus, the significant facts in this proceeding are:

- (1) The '1270 proceeding is in the active examination phase of the proceeding, in which the claim patentability issues have been addressed in the first action, and the proceeding is awaiting examiner action on the response to the Office action³;
- (2) The '1270 proceeding also includes reexamination of claims 10, 12-14, 26 and 28-30, which claims have not been raised in the civil litigation; the proceeding would continue with respect to at least these claims, even if the patentability was finally resolved in the litigation for claims 1, 4, 15, 17, 20, 31, 33, and 35; and
- (3) The district court action has not been made final, and final resolution of the action is not expected in the near future.⁴

These facts, taken with the rest of the facts and circumstances of this case, do not support a finding of good cause to suspend the '1270 proceeding.

The facts in this proceeding are not squarely aligned with the facts in *Sony*. Although all remaining (reexamination proceeding) claims had been litigated and on appeal when the renewed petition to suspend was filed in the proceedings in *Sony*, that was not the only factor considered

³ This was not so in *Sony*, as will be discussed shortly.

⁴ Again, this was not the situation in *Sony*, as will be discussed shortly.

in the decision granting the renewed petition to suspend.⁵ Rather, the Office considered the relative stages of the concurrent appeal and the reexamination proceedings. As noted by the district court in *Sony*, “the PTO correctly concluded that the two ‘races’ between the parties were at very different stages: The Federal Circuit appeal was nearing its conclusion, while the PTO’s *inter partes* review was just beginning.”⁶ The relative stages in this situation are much closer.

In contrast to the *Sony inter partes* reexamination proceedings, which were just at their beginning stages (e.g., the Office’s work had been limited only to a finding that the requests for reexamination had raised a substantial new question of patentability), the present reexamination proceeding has advanced significantly beyond the beginning stage. In this instance, the Office has issued a non-final Office action, in response to which the patent owner has filed a patent owner’s response. Thus, patentability issues have been defined and argued by parties, and the Office’s work in the reexamination proceeding has not been limited to merely finding that the request for reexamination raised a substantial new question of patentability (at which point a patentability determination has not yet been made). On the other hand, the district court case has not yet been made final, as was the case in *Sony*, and has appellate review has not been exhausted.

Additionally, the reexamination proceeding must proceed with special dispatch to resolve the substantial new questions of patentability raised by the reexamination request with respect to claims 10, 12-14, 26 and 28-30, regardless of the outcome of claims 1, 4, 15, 17, 20, 31, 33, and 35 in the civil litigation. The public interest would not be served to suspend the proceeding when there are claims under reexamination that are not subject to a concurrent civil litigation.

Accordingly, good cause for suspension has not been shown, and the Petition under 37 C.F.R. §§ 1.181, 1.182, 1.183 and 1.987 and 35 U.S.C. § 314(c), requesting suspension of the ‘1270 proceeding, is **dismissed**.

As for patent owner’s petition for OPLA to take and retain jurisdiction of the ‘1270 proceeding, OPLA has taken jurisdiction and the decision regarding patent owner’s petitions has now been rendered herein. There is no reason for OPLA to retain jurisdiction for 30 days hence as the patent owner has filed a response and the examiner is prepared to take action. Retaining jurisdiction would serve no useful purpose and would be contrary to the mandate to conduct the proceeding with special dispatch under 35 USC 314(c). Therefore, the petition for OPLA to take and retain jurisdiction is **dismissed**.

CONCLUSION

1. The patent owner petition under 37 C.F.R. §§ 1.181, 1.182, 1.183 and 1.987 and 35 U.S.C. § 314(c) is **dismissed**.

⁵ See the decision entitled “Decision Granting Petitions to Suspend,” mailed on November 17, 2005, in reexamination proceeding control no. 95/000,094.

⁶ *Sony*, 2006 U.S. Dist. LEXIS 36856, at *19.

2. The patent owner petition under 37 C.F.R. § 1.182 for OPLA to take and retain jurisdiction is granted to the extent that OPLA took jurisdiction to decide the patent owner's petitions, and dismissed as to the request that OPLA retain jurisdiction.
3. The third party requester opposition petition under 37 C.F.R. § 1.182 and/or § 1.183 is granted to the extent that is has been entered and considered.
4. Jurisdiction over this proceeding is returned to the Central Reexamination Unit to continue reexamination with special dispatch.
5. The patent owner and the third party requester are respectfully reminded of their continuing duty to keep the Office apprised as to the status of the concurrent litigation pursuant to 37 C.F.R. § 1.985.
6. Any questions concerning this communication should be directed to Caroline D. Dennison, Legal Advisor, at 571-272-7729.

/Kenneth M. Schor/

Kenneth M. Schor
Senior Legal Advisor
Office of Patent Legal Administration

05-11-10
Kenpet8/IP/suspend

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No: 7,188,180)	Reexam Control
)	No.: 95/001,270
Victor LARSON, et al.)	
)	Group Art Unit: 3992
Issued: March 6, 2007)	
)	Examiner: A. Nalven
Filed: November 7, 2003)	
)	Conf. No. 2128
Title: METHOD FOR ESTABLISHING SECURE)	
COMMUNICATION LINK BETWEEN)	
COMPUTERS OF VIRTUAL PRIVATE)	
NETWORK)	

THIRD PARTY REQUESTER'S NOTICE OF NON-PARTICIPATION

Attn: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit (CRU)
Office of Patent Legal Administration
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

An Office Action was mailed in this *Inter Partes* Reexamination on January 19, 2010, and the Patent Owner filed its Response on April 19, 2010.

The Third Party Requester Microsoft Corporation ("the Requester") hereby provides notice to the Patent Office that it will not be filing Comments in response to the January 19, 2010 Office Action and the Patent Owner's April 19, 2010 Response. The Requester provides additional notice that it will not participate further in this *Inter Partes* Reexamination.

Service of Papers

The undersigned certifies pursuant to 37 C.F.R. § 1.903 this Notice paper was served in its entirety on the Patent Owner of record at:

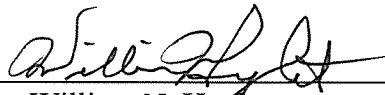
McDermott, Will & Emery, LLP
28 State Street
Boston, MA 02109-1775

on the 18th day of May, 2010.

If any fees are required in connection with this Notice, please charge the same to our Deposit Account No. 02-2135.

Respectfully submitted,

ROTHWELL, FIGG, ERNST & MANBECK, P.C.

By: 
William N. Hugnet
Reg. No. 44,481

1425 K Street, NW
Suite 800
Washington, D.C. 20005
Telephone: (202) 626-3534
Facsimile: (202) 783-6031

Date: May 18, 2010.


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No: 7,188,180)	Reexam Control
)	No.: 95/001,270
Victor LARSON, et al.)	
)	Group Art Unit: 3992
Issued: March 6, 2007)	
)	Examiner: A. Nalven
Filed: November 7, 2003)	
)	Conf. No. 2128
Title: METHOD FOR ESTABLISHING SECURE)	
COMMUNICATION LINK BETWEEN)	
COMPUTERS OF VIRTUAL PRIVATE)	
NETWORK)	

CERTIFICATE OF SERVICE

I hereby certify that the **Third Party Requester's Notice of Non-Participation**, filed May 18, 2010 with the United States Patent and Trademark Office, was served this 18th day of May, 2010 on the Patent Owner by causing a true copy of same to be deposited with Federal Express for delivery to:

VirnetX, Inc.
C/O McDermott, Will & Emery, LLP
28 State Street
Boston, MA 02109-1775



Jessica Fu

Electronic Acknowledgement Receipt

EFS ID:	7638405
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	William Neal Hughet/Jessica Fu
Filer Authorized By:	William Neal Hughet
Attorney Docket Number:	077580-0090
Receipt Date:	18-MAY-2010
Filing Date:	08-DEC-2009
Time Stamp:	18:30:58
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Miscellaneous Incoming Letter	NoticeNonParticipation.pdf	68537 <small>5962a28e6fc2ebfae74353b244b783df86438ac</small>	no	2

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2	Reexam Certificate of Service	CertificateOfService.pdf	23797	no	1
			1fe6c150c9a8c85708c26dbe78a999df1e54b2d2		

Warnings:

Information:

Total Files Size (in bytes):	92334
-------------------------------------	-------

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 the Reexamination of:)	
Victor Larson, et al.)	
)	
U.S. Patent No.: 7,188,180)	
Filed: November 7, 2003)	Examiner:
Issued: March 6, 2007)	Andrew L. Nalven
)	
For: METHOD FOR ESTABLISHING)	Group Art Unit: 3992
SECURE COMMUNICATION LINK)	
BETWEEN COMPUTERS OF VIRTUAL)	
PRIVATE NETWORK)	
)	
Reexamination Proceeding)	
Control No.: 95/001,270)	
Filed: December 8, 2009)	

NOTICE OF RESUBMISSION

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Patent Owner thanks Examiner Nalven for his telephone call of May 19, 2010 in which he requested that Patent Owner resubmit the Response to Office Action in Reexamination filed April 19, 2010 (“Response”) to the U.S. Patent and Trademark Office with a corrected electronic signature.

In accordance this request, Patent Owner hereby resubmits the Response with a proper electronic signature.

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Atabak R. Royae, Reg. No. 59,037
McDermott Will & Emery LLP
Attorneys for Patent Owner
**Please recognize our Customer No. 23630 as
our correspondence address.**

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
Date: May 24, 2010
BST99 1650319-1.077580.0090

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
Edmund Munger, et al.)
)
U.S. Patent No.: 7,188,180)
Filed: November 7, 2003) Examiner:
Issued: March 6, 2007) Andrew L. Nalven
)
For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
SECURE COMMUNICATION LINK)
BETWEEN COMPUTERS OF)
VIRTUAL PRIVATE NETWORK)
)
Reexamination Proceeding)
Control No.: 95/001,270)
Filed: December 8, 2009)

RESPONSE TO OFFICE ACTION IN REEXAMINATION

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Patent Owner hereby responds to the Office Action dated January 19, 2010 (“the Office Action”) in the Reexamination of the above-mentioned patent (“the ‘180 Patent”) having a period of response set to expire on April 19, 2010 in view of the extension of time granted on February 25, 2010.

Remarks begin on page 2 of this response.

REMARKS

Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 Patent are under reexamination, with claims 1, 17, and 33 being independent. Claims 1, 10, 12-15, 17, 26, 28-31, and 33 stand rejected. Claims 4, 20, and 35 are confirmed to be patentable.

Submitted herewith is a Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132 ("Nieh Dec.") in support of the Patent Owner's response.

I. Patent Owner's Response To the Rejection

A. Introduction

The Patent Owner's invention, as defined in independent claim 1, is directed to a method for accessing a secure computer network address. The method comprises the steps of: (i) receiving a secure domain name; (ii) sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name; (iii) receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and (iv) sending an access request message to the secure computer network address using a virtual private network communication link.

The patent provides a technique for establishing a virtual private network ("VPN") communication link between a first computer and a second computer over a computer network. '180 Patent at col. 49, ll. 57-59. To illustrate one non-limiting example, a client computer is connected to a computer network, such as the Internet. *Id.* at col. 50, ll. 1-4. The client computer connects to a server over a non-VPN communication link using a web browser to display a web page. *Id.* at col. 50, ll. 8-25.

According to one variation, the web page can contain a hyperlink for selecting a VPN communication link to the server. *Id.* at col. 50, ll. 25-31. By selecting the hyperlink, a client can secure the communication between itself and the server. *Id.* at col. 51, ll. 5-14. The user need only click the hyperlink – no need to enter user identification information, passwords, or encryption keys. *Id.* Accordingly, in this example, establishing a secure communication link between the user and server are performed transparently to a user. *Id.* To support this transparency, the technique disclosed in the '180 Patent provides for automatically replacing the

Control Number: 95/001,270

top-level domain name of the server within the web browser with a secure top-level domain name for the server. *Id.* at col. 51, ll. 15-28. For example, if the top-level domain name for the server is “.com,” it may be replaced with “.scom”. *Id.*

Because a secure top-level domain name can be a non-standard domain name, a query to a standard domain name system (“DNS”) would return a message indicating that the universal resource locator (“URL”) is unknown. *Id.* at col. 51, ll. 28-35. Therefore, according to the patent, the query can be sent to a secure domain name service for obtaining the URL for the secure top-level domain name. *Id.* The secure domain name service can contain a cross-reference database of secure domain names and corresponding secure network addresses. *Id.* at col. 52, ll. 4-26. That is, for each secure domain name, the secure domain name service stores a computer network address corresponding to the secure domain name. *Id.* An entity can register a secure domain name in the secure domain name service so that a user who desires a secure communication link to the web site of the entity can automatically obtain the secure computer network address for the secure website. *Id.* An entity can also register several secure domain names, with each respective secure domain name representing a different priority level of access to the secure website. *Id.*

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. *Id.* 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. *Id.* When a user queries the secure domain name service for the secure computer network address for the securities trading website, the secure domain name service determines the particular secure computer network address based on the user's identity and the user's subscription level. *Id.*

B. Applicable Standards for Rejection

1. Applicable Standard for Rejection Under 35 U.S.C. § 102

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102. A rejection under 35 U.S.C. § 102 requires that “each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *See* MPEP § 2131, citing *Verdegaal Bros. v. Union Oil Col. of California*, 814 F.2d

Control Number: 95/001,270

628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The above-stated rejection, however, fails to meet this standard.

2. Applicable Standard for Rejection Under 35 U.S.C. § 103(a)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent also stand rejected under 35 U.S.C. § 103(a). In reconsidering the outstanding 35 U.S.C. § 103(a) rejections, the Examiner must consider any evidence supporting the patentability of the claimed invention, such as any evidence in the specification or any other evidence submitted by the Patent Owner, such as the secondary considerations of non-obviousness submitted herewith. The ultimate determination of patentability is based on the entire record, by a preponderance of evidence, which requires the evidence to be more convincing than the evidence which is sought in opposition to it. *See* MPEP § 2142 (citing *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992)).

Each of the rejections under 35 U.S.C. § 103(a) fails to meet these standards by a preponderance of the evidence.

3. Applicable Standard for Demonstrating a Publication Date

As identified below, a number of references have not been shown to qualify as prior art to the '180 Patent. The Office Action and the Request for *Inter Partes* Reexamination of Patent ("Request") both fail to demonstrate the actual publication date of various of the relied upon references necessary to establish a *prima facie* showing that each reference is prior art. The Patent Owner is left to assume that the assertion that the references are prior art arises from the copyright date printed on the face of each reference. This copyright date is not, however, the 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, 226 (C.C.P.A. 1981). Unlike a publication date, a copyright date merely establishes "the date that the document was created or printed." *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 975 (E.D. Mich. 2003).

Presuming the author of a document accurately represented the date the document was created, this creation date is not evidence of any sort of publication or dissemination. Without

Control Number: 95/001,270

more, a 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.

The party asserting the prior art bears the burden of establishing a date of publication. *See Carella v. Starlight Archery*, 804 F.2d 135, 139 (Fed. Cir. 1986) (finding that a mailer did not qualify as prior art because there was no evidence as to when the mailer was received by any of the addresses). Here, the Office bears the burden of establishing a prima facie case of unavailability, including that the references relied upon are proper prior art. *See In re Hall*, 781 F.2d 897 (Fed. Cir. 1986) (Affidavits on public availability of a reference were necessary for the Examiner to establish the reference to be prior art.). Yet, neither the Office Action nor the Request even attempt to show that various of the references identified below were disseminated or made publicly available.

Thus, the Patent Owner respectfully submits that, as demonstrated below, a number of references relied upon in the Office Action have not been shown to be prior art to the rejected claims. Accordingly, the Patent Owner respectfully requests that the rejections over these references be withdrawn.

C. The Rejection of Claims Over Alleged Prior Art

The outstanding rejections rely on the erroneous premise that the “secure domain name” and “secure domain name service” recited in independent claims 1, 17, and 33 of the ‘180 Patent are a standard domain name and domain name service, respectively. In the interest of brevity, the Patent Owner here reveals the fault in this premise by outlining the differences here at the outset and refers back to these statements when addressing each rejection of the Office Action below.

The Request and Office Action rely on the erroneous premise that a secure domain name is a domain name that happens to correspond to a secure computer. *See, e.g.*, Office Action at 6; Request at 15. Alternatively, the Request and Office Action rely on the faulty position that a secure domain name corresponds to an address that simply requires authorization. Request at 21. These assertions are in clear contradiction to the specification of the ‘180 Patent, which takes pains to explain that a secure domain name is different from a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization. *Id.*; ‘180 Patent at col. 51, ll. 18-28; Nieh Dec. at ¶ 10. To illustrate, in various

Control Number: 95/001,270

implementations, the '180 Patent describes that a secure domain name is a "a non-standard domain name." '180 Patent at col. 51, ll. 29-31; Nieh Dec. at ¶ 10. Examples of such non-standard domain names are described in Claim 11: .scom, .snet, .sorg, .sedu, .smil, and .sgov. Nieh Dec. at ¶ 10. Dependent claim 2 also differentiates between a secure domain name and a non-secure domain name in reciting the step of "automatically generating a secure domain name corresponding to a non-secure domain name." *Id.* To further illustrate, the '180 Patent describes that "a query [with a secure domain name] to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." *Id.*; '180 Patent at col. 51, ll. 28-32. Thus, the Patent Owner respectfully submits that the inventors of the '180 Patent acted as their own lexicographers in providing that the secure domain name recited in claims 1, 17, and 33 of the '180 Patent cannot be properly read to be a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization. Nieh Dec. at ¶ 10. As seen from the previous sentences, a secure domain name is different from a domain name that just happens to be associated with a secure computer or secure computer network address. For example, as pointed above, the domain name that just happens to correspond to a secure computer or a domain name that just happens to correspond to an address requiring authentication can be resolved, for example, by a conventional domain name service; whereas, as noted above, a secure domain name cannot be resolved by a conventional domain name service, for example. *Id.*

Furthermore, the Patent Owner notes that even if the recitation "secure domain name" is defined according to the Request to mean a domain name corresponding to a secure computer or a domain name corresponding to an address requiring authorization, various of the cited documents still fail to describe or suggest this feature. Nieh Dec. at ¶ 11. Specifically, the relied upon portions of the cited documents describe domain names of computers that do not require authorization for access. Instead, the computers (*e.g.*, a VPN tunnel server or a PPTP server) of the cited documents are for securing a connection between a client computer and a target computer. *Id.* To this end, the computers (*e.g.*, a VPN tunnel server or a PPTP server) themselves do not have a secure computer network address because they do not require authorization for access or authorization for a client computer to communicate with them. *Id.* Any client computer can without authorization communicate with one of these computers (*e.g.* a VPN tunnel server or a PPTP server); it is the target computer that may requires authorization for

Control Number: 95/001,270

access. *Id.* Therefore, neither the domain name of the computers (*e.g.*, a VPN tunnel server or a PPTP server) nor their corresponding computer network address is secure – even if this term is defined according to the Request. *Id.* As such, these cited documents do not teach a secure computer network address or, correspondingly, a secure domain name.

Similarly, the Request and Office Action rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of secure computers. *See, e.g.*, Office Action at 7; Request at 15. Alternatively, the Request and Office Action also rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of computers that are used to establish a secure connection, such as a VPN tunnel server or a PPTP server. *See, e.g.*, Office Action at 16; Request at 21. Again, these arguments are belied by the ‘180 Patent itself. The specification of the ‘180 Patent clearly teaches that the claimed secure domain name service is unlike a conventional domain name service, which the inventors understood as including both DNS and DNS with public key security. Nieh Dec. at ¶ 12; *see* col. 51, ll. 29-45; col. 52, ll. 4-26. To illustrate, the ‘180 Patent explicitly states 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. *See*, ‘180 Patent at col. 51, ll. 18-45 (stating “[b]ecause 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”); Nieh Dec. at ¶ 12. A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name. Nieh Dec. at ¶ 12. A secure domain name service of the ‘180 Patent, instead, recognizes that a query message is requesting a secure computer network address and performs its services accordingly. Nieh Dec. at ¶ 12. Furthermore, in various implementations, the ‘180 Patent describes a secure domain name service as providing additional functionalities not available with a traditional domain name service, as described above in Section I.A. and in the ‘180 Patent at col. 52, ll. 4-26. *Id.* The ‘180 Patent even describes the drawbacks of the conventional scheme of traditional DNS and public key security:

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

Control Number: 95/001,270

automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).

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

'180 Patent at col. 40, ll. 6-17; Nieh Dec. at ¶ 12. Thus, the Patent Owner respectfully submits that the secure domain name service recited in claims 1, 17, and 33 of the '180 Patent is different from a conventional domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

1. The Rejection of Claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 Under 35 U.S.C. § 102(a) in view of Aventail Connect v3.1/v2.6 Administrator's Guide (hereafter "Aventail")

Claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 of the '180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Aventail. The rejection is based on the reasons given on pages 12-19 of the Request, Appendix A to the Request, and the additional reasons presented on pages 6-12 of the Office Action. The Patent Owner respectfully traverses this rejection because (i) Aventail has not been shown to be prior art under § 102(a) and (ii) assuming, *arguendo*, that Aventail qualifies as prior art, Aventail has not been shown to teach, either expressly or inherently, each and every element of independent claims 1, 17, and 33. The following remarks address each of these points in turn.

a) Aventail has not been shown to be prior art under § 102(a)

Both the Office Action and the Request assert that Aventail was published between 1996 and 1999 without any stated support. Request at 5; Office Action at 2. The Patent Owner can only presume that this assertion arises from the copyright date range printed on the face of the reference: "© 1996-1999 Aventail Corporation." See Aventail at *i*. As stated in Section I.B.3., above, this copyright date range is not the publication date of Aventail and the Office Action has failed to make any showing that it is.

Further, the closeness of proximity of the alleged publication date of Aventail to the April 26, 2000 priority date of the '180 Patent raises further doubt as to the availability of Aventail as prior art. Suppose the relied upon sections of the Aventail reference were created on December

Control Number: 95/001,270

31, 1999, and the copyright date range accordingly amended to read “1996-1999.” Under these circumstances, it is possible that the document was not disseminated until after the filing date of the ‘180 Patent, a mere four months later. Under these circumstances, Aventail clearly would not be eligible to be relied upon as prior art to the ‘180 Patent.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Aventail is prior art and requests all rejections based on Aventail be withdrawn. Nonetheless, the Patent Owner addresses Aventail below as though it is qualified prior art.

b) Aventail has not been shown to teach each and every element of independent claims 1, 17, and 33

(1) Aventail fails to teach “a secure domain name” and “a secure domain name service”

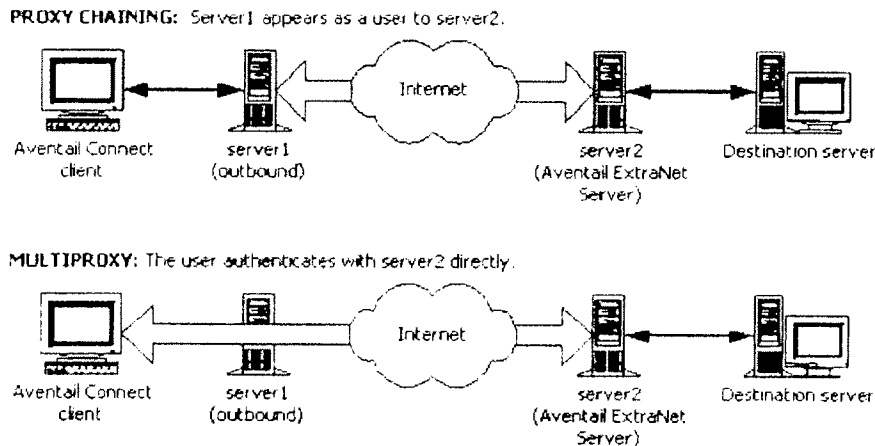
First, Aventail fails to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Aventail discloses a system and architecture for transmitting data between two computers using the SOCKS protocol. Nieh Dec. at ¶ 14. The system routes certain, predefined network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, possibly through successive servers. Aventail at 7; Nieh Dec. at ¶ 14. Upon receipt of the network traffic, the SOCKS server transmits the network traffic to the Internet or external network. Aventail at 7; Nieh Dec. at ¶ 14. Aventail’s disclosure is limited to connections created at the socket layer of the network architecture. Nieh Dec. at ¶ 14.

In operation, Aventail discloses that a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. Aventail at 9; Nieh Dec. at ¶ 15. The Aventail Connect software is disclosed to intercept 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 Dec. 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 Dec. 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 Dec. at ¶ 16. The SOCKS server performs the hostname resolution. Aventail at 12; Nieh Dec. at ¶ 17. Once the hostname is resolved, the user can transmit data over

Control Number: 95/001,270

a SOCKS connection to the SOCKS server. Nieh Dec. at ¶ 17. The SOCKS server, then, separately relays that transmitted data to the target. *Id.*

Along with this basic operation, the Request cites to a “Proxy Chaining” and a “MultiProxy” mode disclosed in Aventail. Request at 12; Aventail at 68-73. In the “Proxy Chaining” mode, Aventail discloses that a user can communicate with a target via a number of proxies such that each proxy server acts as a client to the next downstream proxy server. Aventail at 68; Nieh Dec. at ¶ 18. As shown below, in this mode, the user does not communicate directly with the proxy servers other than the one immediately downstream from it. Aventail at 68, 72; Nieh Dec. at ¶ 18.



Aventail at 72. In the “MultiProxy” mode, Aventail discloses that the user, via Aventail Connect, connects through each successive proxy server directly. Aventail at 68; Nieh Dec. at ¶ 20. Regardless of whether one of these modes is enabled, the operation of Aventail Connect does not materially differ between the methods. Nieh Dec. at ¶ 21.

Nowhere in these teachings does Aventail teach a secure domain name. The Office Action asserts that the hostname (e.g., the alleged secure domain name) is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption. Office Action at 6. To this end, the Office Action interprets a secure domain name as a domain name associated with a secure computer. *Id.* As stated above at the beginning of Section I.C., which is incorporated herein by reference, this assertion is incorrect. *See also* Nieh Dec. at ¶ 22.

Similarly, Aventail has not been shown to teach a secure domain name service. The Office Action suggests that a DNS server that can resolve addresses of secure computers

Control Number: 95/001,270

corresponds to a secure domain name service. *See*, Office Action at 7. This is incorrect. Aventail has not been shown to teach anything more than a conventional DNS. Nieh Dec. at ¶ 23. As stated above in the beginning of Section I.C., a secure domain name service is not a conventional domain name service. *Id.* A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

The Request has not shown Aventail to disclose a domain name service other than a traditional domain name service. The Request asserts that Aventail discloses two look-up services, alleged to be described on pages 8 and 12 of that reference. Request at 15. On page 8, Aventail discloses the traditional protocol for a computer to connect to a remote host. Nieh Dec. at ¶ 24. On page 12, Aventail discloses “forward[ing] the host-name to the extranet (SOCKS) server [where] the SOCKS server performs the hostname resolution.” *Id.* Thus, Aventail has not been shown to disclose anything other than a traditional DNS. *Id.* As noted above at the outset of Section I.C., a secure domain name service is unlike a conventional domain name service. *Id.* A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

For at least these reason, Aventail fails to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of independent claims 1, 17, and 33 and the rejected dependent claims 10, 12, 14, 26, 28, 30, and 31.

(2) Aventail fails to teach “a virtual private network link”

Aventail has not been shown to teach sending an access request message to a secure computer network address using a virtual private **network** communication link, as recited in claims 1, 17, and 33.

The links created by the systems and methods disclosed in Aventail differ from the virtual private network communication link recited in claims 1, 17, and 33. Nieh Dec. at ¶ 25. 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.* Aventail discloses establishing point-to-point SOCKS connections between a client computer

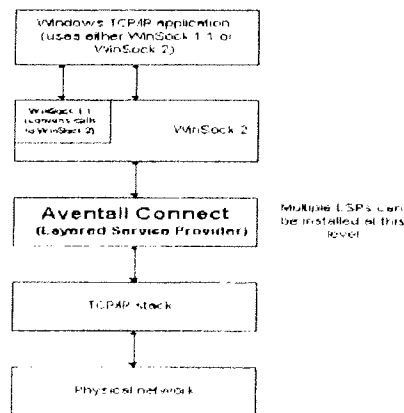
Control Number: 95/001,270

and a SOCKS server. *Id.* The SOCKS server then relays data received to the intended target. *Id.* Aventail does not disclose a virtual private network, as recited in claims 1, 17, and 33, 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 virtual private network. *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 virtual private network. *Id.*

Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users transmitting data that is 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:



Control Number: 95/001,270

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.* at ¶ 28. Thus, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33. *Id.*

Third, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33, 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 at least the foregoing reasons, Aventail fails to describe or suggest sending an access request message to the secure computer network address using a virtual private network communication link, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of independent claims 1, 17, and 33, along with their dependent claims 10, 12, 14, 26, 28, 30 and 31.

2. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 103(a) in view of Microsoft Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview") and RFC 1035

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent stand rejected under 35 U.S.C. § 103(a) as being unpatentable over VPN Overview in view of RFC 1035. The rejection is based on the reasons given on pages 19-25 and Appendix B of the Request. The Patent Owner respectfully traverses this rejection because (i) VPN Overview has not been shown to be prior

Control Number: 95/001,270

art, and (ii) assuming, *arguendo*, that VPN Overview qualifies as prior art, VPN Overview and RFC 1035, alone or in combination, have not been shown to teach, either expressly or inherently, each and every element of each of the independent claims 1, 17, and 33. The following remarks address each of these points in turn.

a) VPN Overview has not been show to qualify as prior art.

Both the Office Action and the Request assert that VPN Overview was published in 1998 without any stated support. Request at 5; Office Action at 2. The Patent Owner can only presume that these assertions arise from the copyright year printed on the face of the reference. *See*, VPN Overview at 2. As stated in Section I.B.3., above, this copyright date range is not the publication date of VPN Overview and the Office Action has failed to make any showing that it is. Indeed, the document is on its face identified as nothing more than a draft. VPN Overview at 1 (Stating the following: “White Paper – DRAFT”).

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that VPN Overview is prior art and requests all rejections based on VPN Overview be withdrawn. Nonetheless, the Patent Owner addresses VPN Overview below as though it is qualified prior art.

b) VPN Overview and RFC 1035 fail to teach, either expressly or inherently, each and every element of independent claims 1, 17, and 33 and fail to render those claims obvious.

VPN Overview and RFC 1035, either alone or in the proposed combination, fail to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33.

Here, VPN Overview provides an overview of VPNs, describing their basic requirements, and some of key technologies that permit private networking over public networks. *See*, VPN Overview at Abstract; Nieh Dec. at ¶ 30. For example, referring to FIG. 2 of VPN Overview, shown below, a VPN is shown to connect a remote user to a corporate Intranet. VPN Overview at 7; Nieh Dec. at ¶ 30. VPN Overview at 7. To this end, a user calls a local ISP and using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet. *See* VPN Overview at 8; Nieh Dec. at ¶ 30.

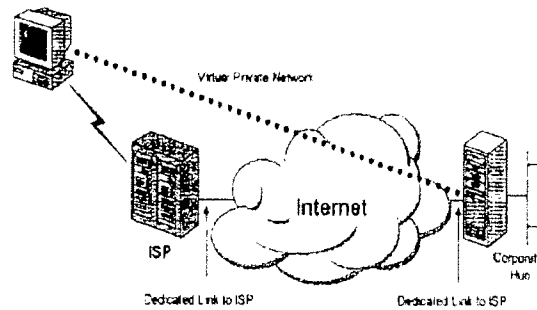


Figure 2. Using a VPN to connect a remote client to a private LAN

The Request asserts that a VPN tunnel server of the VPN Overview system can be identified using a domain name. Request at 21 (citing VPN Overview at page 26 asserting that the VPN tunnel server can be named “vpn.x.support.bigcompany.com”). The Request concludes and alleges that this domain name corresponds to a secure domain name because the domain name corresponds to a network address that requires authorization. *See* Request at 21. The Patent Owner respectfully disagrees for several reasons.

VPN Overview provides no indication that the client is sending a domain name to the Front End Processor (“FEP”) to establish a connection; instead, the indication is that the client is establishing a dial-up connection to the FEP. VPN Overview at 22 (stating “[i]n the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP.”); Nieh Dec. at ¶ 31. Even assuming for the sake of argument that the alleged domain name is sent from the client to the FEP, the VPN Overview provides no evidence that the alleged domain name is a secure domain name in the context of this application. Nieh Dec. at ¶ 31. A secure domain name, as recited in claim 1, 17, and 33 of the ‘180 Patent, is not a domain name that just happens to be associated with a computer used to establish a secure connection, as identified above at the outset of Section I.C. The Request alleges that VPN Overview describes a secure domain name because the domain name for the VPN tunnel server happens to correspond to a network address allegedly requiring authentication. *Id.* at ¶ 31. As stated at the outset of Section I.C., above, however, a secure domain name is not a domain name that so happens to correspond to a network address for a server involved in securing communications. *Id.*

The domain name of the VPN tunnel server is also not a secure domain name, even if this recitation is incorrectly defined according to the Request. *Id.* at ¶ 32. The Request asserts that a secure domain name corresponds to a secure computer network address. *Id.* However, the

Control Number: 95/001,270

address of the VPN tunnel server is not a secure computer network address, as stated above at the beginning of Section I.C. *Id.* Assuming for the sake of argument that a secure computer network address is associated with a computer which requires authorization for access, then, without authorization for access, a client computer cannot communicate with a secure computer network address. *Id.* In VPN Overview, however, a client computer may communicate with a VPN tunnel server without pre-authorization to access the hosts protected by the VPN tunnel server. *Id.* Thus, because the VPN tunnel server of the reference does not require authorization for access, it is not associated with a secure computer network address, and therefore also cannot be associated with a secure domain name. *Id.*

VPN Overview also has not been shown to teach or suggest a secure domain name service, as recited in claims 1, 17, and 33. VPN Overview, on page 26, describes that redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. *Id.* at ¶ 33. The round-robin DNS, however, is no different from a conventional DNS. *Id.* As stated above at the outset of Section I.C., a secure domain name service is not a conventional DNS. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

The Request appears to recognize these shortcomings of VPN Overview and therefore relies on RFC 1035 to supplement that reference. RFC 1035 is equally deficient. The Patent Owner respectfully submits that the proposed combination of VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name and a secure domain name service as recited in claims 1, 17, and 33. *Id.* at ¶ 34.

RFC 1035 describes user programs that interact with the domain name space through resolvers; the format of user queries and user responses is specific to the host and its operating system. RFC 1035 at 4; Nieh Dec. at ¶ 34. User queries will typically be operating system calls, and the resolver and its cache will be part of the host operating system. RFC 1035 at 4; Nieh Dec. at ¶ 34. Resolvers answer user queries with information they acquire via queries to foreign name servers and the local cache. RFC 1035 at 4; Nieh Dec. at ¶ 34.

Even assuming for the sake of the argument that this description supports the allegation that the user query corresponds to a domain name and the resolver corresponds to a domain name

Control Number: 95/001,270

service, RFC 1035 still fails to describe or suggest a secure domain name and a secure domain name service, as outlined at the outset of Section I.C., above. Nieh Dec. at ¶ 35. RFC 1035 is not seen to show anything other than a conventional DNS. *Id.* The Request also points to no evidence that distinguishes the alleged DNS of RFC 1035 from a conventional DNS. *Id.* at ¶ 36. Instead, the Request merely states that RFC 1035, on page 22, discloses that the domain name is sent to a domain name service for resolution and then passed back the IP address. Request at 22; *id.* As stated above in Section I.C., a secure domain name service unlike a conventional DNS. *Id.* Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.* As such, the proposed addition of subject matter from RFC 1035 fails to remedy the shortcomings of VPN Overview to describe or suggest a secure domain name or secure domain name service, as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 36.

Furthermore, the proposed combination of the VPN Overview and RFC 1035 also fails to describe or suggest a secure domain name or a secure domain name service even if these recitations are incorrectly defined as suggested by the Request. *Id.* at ¶ 37. The Request asserts that the secure domain name corresponds to a secure computer network address, and a secure domain name service corresponds to a lookup service that returns a secure network address for the requested secure domain name. Request at 21, 22. The proposed combination of the VPN Overview and RFC 1035 in fact does not teach these features. Nieh Dec. at ¶ 37.

The proposed combination of the VPN Overview and RFC 1035, at best, shows a DNS server that can allegedly receive the domain name of the VPN tunnel server and can allegedly resolve and return the IP address for the domain name of the VPN tunnel server. *Id.* at ¶ 38. As noted above, the issue is that the purpose of the VPN tunnel server is to secure a connection to resources behind the VPN tunnel server. *Id.* To this end, the VPN tunnel server itself is not secure – that is, it does not require authorization for access, as stated above at the outset of Section I.C. *Id.* Therefore, neither the domain name of the VPN tunnel server nor its corresponding computer network address is secure – even if this term is incorrectly defined as proposed by the Request. *Id.* As such, even under the Requester’s claim interpretation, the proposed combination of the VPN Overview and RFC 1035 fails to describe or suggest a secure domain name or a secure domain name service. *Id.*

As such, the proposed combination of the VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 39. For at least the foregoing reasons, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of independent claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

c) Secondary Considerations of Non-Obviousness

The Patent Owner presents in the §1.132 Declaration of Edmund Munger submitted herewith (“Munger Dec.”), objective evidence of non-obviousness of the rejected claims and a nexus between that evidence and the claimed inventions. This evidence is entitled to great weight as evidence of non-obviousness.

Perhaps most revealing is the jury verdict against the Requestor, Microsoft Corporation, finding that each of the independent claims here rejected, as well as some dependent claims, were not invalid and were willfully infringed by the Requester. Munger Dec. at ¶ 4. The jury awarded the Patent Owner **thirty four million dollars (\$34,000,000)** in damages stemming from infringement of the ‘180 Patent, including the independent claims rejected by the Office Action. *Id.* at ¶ 4. Because the rejected claims were found willfully infringed, the nexus is undeniable. The damage award is significant and clearly evinces significant commercial success.

Microsoft was not the only one seeing value in the claimed invention. SafeNet, a leading provider of Internet security technology that is the *de facto* standard in the VPN industry, entered into a portfolio license (which included the technology that became covered by the claims of the ‘180 Patent) in July 2002 to be incorporated into SafeNet’s VPNs. *Id.* at ¶ 12.

Considering the need for easy-to-use Internet security at the time of invention, the value of these inventions is not surprising. In 1998, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks. *Id.* at ¶ 10. In that time period, remote access was “a nightmare for support desks. Staffers never know what combination of CPU, modem, operating system and software configuration they’re going to have to support”, and adding the commercially available VPN software only made matters worse. *Id.* The computer and internet security industries were forced to chose between the ease of use and the security that the VPN system provided. *Id.* The inventions defined by claims 1, 17, and 33 of

Control Number: 95/001,270

the '180 Patent, combine both the ease of use and security aspects of a VPN, without sacrificing one or the other. *Id.*

In fact, prior to the invention of claims 1, 17 and 33 of the '180 Patent, there was significant and increasing concern with the security of computer communications. *Id.* at ¶ 5. In one example, the Defense Advanced Research Projects Agency ("DARPA") provided significant funding for development of Internet security. DARPA provided funding of approximately \$130,000,000 from 1998 through 2000 alone. At least fifteen 15 different organizations were working on research, but none of them came up with the solution defined by claims 1, 17, and 33 of the '180 Patent. *Id.* at ¶ 7. In another example, In-Q-Tel, a company with strong ties to the U.S. CIA, funded the original development of secure remote connections technology to the tune of \$3,400,000. *Id.* at ¶ 8.

Recognizing the long felt need for these inventions, the original owner of the '180 Patent spent significant resources on their development. In fact, in the year the inventions were developed, it spent an amount in the development of these inventions nearly equal to its entire research and development budget for that year. *Id.* at ¶ 9.

The Examiner "must" consider secondary evidence of non-obviousness. MPEP 716.01(a). Such evidence is "often...the most probative and cogent evidence" of non-obviousness. *Demaco Corp. v. F. Von Langsdorff Licensing*, 851 F.2d 1387, 1391 (Fed. Cir. 1988). Secondary indicia of non-obviousness is entitled to "substantial weight" in the obviousness analysis when the Patent Owner establishes a nexus between the evidence and the claimed invention. *Stratoflex Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1539 (Fed. Cir. 1983).

For these additional reasons, the Patent Owner respectfully requests the withdrawal of the obviousness rejections of independent claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31 of the '180 Patent.

3. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(b) in view of Kosiur, "Building and Managing Virtual Private Networks" (hereafter "Kosiur")

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent stand rejected under 35 U.S.C. § 102(b) as being anticipated by Kosiur. The rejection is based on the reasons given on pages 25-30 and Appendix C of the Request. The Patent Owner respectfully traverses this

Control Number: 95/001,270

rejection because Kosiur has not been shown to either expressly or inherently teach each and every element of each of the independent claims 1, 17, and 33.

Kosiur has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in each of claims 1, 17, and 33. Nieh Dec. at ¶ 40. Kosiur describes protecting external access to a company's intranet by establishing two corporate DNS servers: one external to the firewall and one internal. Kosiur at 295, 296; *Id.* The external corporate DNS includes a list of hosts that the company permits the public to access, such as, for example, the company's e-mail gateway, public web site, and anonymous FTP server. Kosiur at 296; Nieh Dec. at ¶ 40. The internal corporate DNS includes a list of hosts that only the company's internal network users are permitted to access. Kosiur at 296; Nieh Dec. at ¶ 40. When an internal host attempts to access an external host, the internal DNS server forwards the DNS request to the external DNS server. Kosiur at 296; Nieh Dec. at ¶ 40. In the reverse, however, if an external host attempts to access an internal host, then the external host must connect to the internal DNS server through a VPN. Kosiur at 296; Nieh Dec. at ¶ 40.

Although Kosiur describes a domain name, it does not describe a secure domain name, as recited in claims 1, 17, and 33. The Request asserts that Kosiur discloses domain name usage with VPN enabled servers and computers. *See* Request at 27. These domain names, the Request asserts, are "secure" because the domain names correspond to a network address that requires authentication. *See id.* This is incorrect. Nieh Dec. at ¶ 41. The Patent Owner respectfully submits that such a reading of a claim is contrary to its meaning and reads out a critical aspect of the invention. As identified at the outset of Section I.C., above, a secure domain name is not a domain name that just happens to correspond to a network address that requires authentication. Nieh Dec. at ¶ 41.

Kosiur has also not been shown to disclose a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 42. The Request alleges that a secure domain name service is a look-up request to a domain name service to resolve a domain name identifying VPN resources. Request at 27; Nieh Dec. at ¶ 42. Kosiur describes an internal DNS and an external DNS for resolving addresses of internal hosts and external hosts respectively. Request at 27; Nieh Dec. at ¶ 42. Kosiur has not been shown to disclose that either the internal or external DNS is different from a conventional DNS. Nieh Dec. at ¶ 42. Further, the Request provides no evidence that the DNS disclosed by Kosiur is different from conventional DNS. *Id.* The Request simply states

Control Number: 95/001,270

that “Kosiur discloses at pages 293-296 that domain name resolution occurs at DNS servers. The DNS servers pass back the corresponding network address.” Request at 28; Nieh Dec. at ¶ 42. Thus, Kosiur has not been shown to disclose anything other than a conventional DNS, and, as stated in Section I.C., above, a secure domain name service is not a conventional domain name service. Nieh Dec. at ¶ 42. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. Nieh Dec. at ¶ 42.

As such, Kosiur has not been shown to teach a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 43. For at least the foregoing reasons, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

4. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(a) in view of Kaufman, “Implementing IPsec” (hereafter “Kaufman”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Kaufman. The rejection is based on the reasons given on pages 30-35 and Appendix D of the Request. The Patent Owner respectfully traverses this rejection because Kaufman has not been shown to either expressly or inherently teach each and every element of each of the independent claims 1, 17, and 33.

Kaufman has not been shown to teach a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. Kaufman discloses the use of IPsec to secure communications through the Internet using authentication and encryption. Kaufman at 2; Nieh Dec. at ¶ 44. Kaufman also describes a domain name service being an integral part of the Internet and of any normal IP network. Kaufman at 128; Nieh Dec. at ¶ 44. The domain name service is described as a protocol used to support hierarchical resolution of host names to IP addresses (and vice versa) in the Internet. Kaufman at 243; Nieh Dec. at ¶ 44. Kaufman also describes that a layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Kaufman at 142; Nieh Dec. at ¶ 44. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network. Kaufman at 142; Nieh Dec. at ¶ 44.

Control Number: 95/001,270

Based on the foregoing, the Request alleges that an IPsec connection request over the Internet for a secured resource can use, for example, a DNS server to resolve the request. Request at 31; Nieh Dec. at ¶ 44. Even assuming, *arguendo*, this assertion is correct, it falls short of describing a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 44.

Kaufman has not been shown to teach or disclose a secure domain name, as recited in claims 1, 17, and 33. *Id.* at ¶ 45. Similar to previous assertions, the Request suggests that Kaufman describes a secure domain name simply because it describes a domain name corresponding to a network address involving security (*e.g.*, a computer protected by a home network). *Id.* As stated at the outset of Section I.C., above, however, a secure domain name cannot be properly read to be a domain name that just happens to be associated with a computer network address requiring authentication because this interpretation is inconsistent with the meaning adopted by the inventors of the '180 Patent. *Id.*

Second, Kaufman also has not been shown to describe or suggest a secure domain name service, as recited in claims 1, 17, and 33. The Request alleges that a “‘secure domain name service’ includes any lookup service that resolves a secure domain name.” Request at 32; Nieh Dec. at ¶ 46. Assuming, *arguendo*, that Kaufman discloses a secure domain name, Kaufman has not been shown to disclose a secure domain name service because it has only been shown to disclose a conventional DNS. Nieh Dec. at ¶ 46. As stated at the outset of Section I.C., above, however, a secure domain name service is not a conventional DNS. *Id.* Specifically, a secure domain name service is unlike a conventional DNS that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. *Id.*

Moving forward, the Request also seems to allege that Kaufman’s disclosure of DNS Security (“DNSSEC”) is a secure domain name service. Request at 33; Nieh Dec. at ¶ 47. To the extent Kaufman even discloses DNSSEC, that protocol merely teaches protecting the integrity of the traditional DNS resolution process. Nieh Dec. at ¶ 47. This “conventional scheme” of protecting the integrity of DNS resolution is also explicitly disclosed in column 40, lines 6-14 of the specification of the '180 Patent as being conventional:

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

Control Number: 95/001,270

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).

As noted above, the inventors had explicitly contemplated this “conventional scheme” of performing DNS resolution, and nevertheless claimed a secure domain name service as being something different. Nieh Dec. at ¶ 47. The addition of security to protect the integrity of a traditional DNS look-up, does not teach a secure domain name service for the same reasons as identified at the outset of Section I.C. *Id.* at ¶ 47.

As such, Kaufman has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. *Id.* at ¶ 48. For at least the foregoing reasons, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of claims 1, 17, and 33 and dependent claims 10, 12-15, 26, and 28-31.

5. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 103(a) In View of Kaufman and James M. Galvin, “Public Key Distribution with Secure DNS” (hereafter “Galvin”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 103(a) as being obvious over Kaufman in view of Galvin. The rejection is based on the reasons given on pages 36-41 and Appendix E of the Request.

a) Kaufman and Galvin fail to teach, either expressly or inherently, each and every element of independent claims 1, 17, and 33 and fail to render those claims obvious.

The Patent Owner respectfully submits that neither Kaufman nor Galvin, individually or in combination, describe or suggest each and every element of each of the independent claims 1, 17, and 33. Kaufman’s teachings and deficiencies are identified immediately above in Section I.C.4. Galvin is cited to teach “a second type of ‘secure domain name service’ that includes digitally signed resource records.” Request at 38. Galvin discloses using a public key in the DNS resolution process to protect the integrity of the process. Galvin at §§ 1 and 3.2; Nieh Dec. at ¶ 50. This “conventional scheme” protecting the integrity of DNS resolution is also explicitly disclosed in the specification of the ‘180 Patent:

Control Number: 95/001,270

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).

Col. 40, ll. 6-14; Nieh Dec. at ¶ 50. Thus, the inventors had explicitly contemplated this “conventional scheme” of performing DNS resolution, and nevertheless claimed a secure domain name service as something different. *Id.*

Therefore, this aspect of Galvin does not teach the “secure domain name service” recited in claims 1, 17, and 33. Nieh Dec. at ¶ 51. The Request assumes that a “secure domain name service” is a conventional domain name service which issues a public key to ensure that the service is trustworthy. Request at 36; Nieh Dec. at ¶ 51. As stated above at the outset of Section I.C., disclosure of a conventional domain name service does not disclose a secure domain name service. *Id.* The addition of a public key to ensure the integrity of a DNS look-up does not teach a secure domain name service. *Id.* Accordingly, Galvin fails to remedy the shortcomings of Kaufman to describe or suggest a secure domain name service as recited in claims 1, 17, and 33. *Id.* Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

b) Secondary Considerations of Non-Obviousness

For the reasons stated in Section I.C.2.c above, it would not have been obvious to combine Kaufman and Galvin in the manner proposed in the Office Action. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

6. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(a) in View of Gauntlet® Firewall for Windows NT Administrator’s Guide Version 5.0 (hereafter “Gauntlet”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Gauntlet. The rejection is based on the reasons given on

Control Number: 95/001,270

pages 40-45 and Appendix F of the Request. The Patent Owner respectfully traverses this rejection because (i) Gauntlet has not been shown to be prior art under § 102(a) and (ii) even if it is assumed for the sake of argument that Gauntlet qualifies as prior art, Gauntlet has not been shown to either expressly or inherently teach each and every element of each of the independent claims 1, 17, and 33. The following remarks address each of these points in turn.

a) Gauntlet has not been shown to be prior art under § 102(a).

Both the Office Action and the Request assert that Gauntlet was published between 1998 and 1999 without any stated support. Request at 6; Office Action at 3. The Patent Owner can only presume that this assertion arises from the copyright date range printed on the face of the reference. *See* Gauntlet at *ii*. As stated in Section I.B.3., above, this copyright date range is not the publication date of Gauntlet and the Office Action has failed to make any showing that it is.

The closeness of proximity of the alleged publication date of Gauntlet to the April 26, 2000 priority date of the '180 Patent makes the availability of the reference even more dubious. Suppose the relied upon sections of the Gauntlet reference were created on December 31, 1999, and the copyright date range was accordingly amended to read "1998-1999." Under these circumstances, it is possible that the document, although created, was not disseminated until after the April 26, 2000, four months after creation. Under these circumstances, Gauntlet clearly would not be eligible to be relied upon as prior art to the '180 Patent.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Gauntlet is prior art and requests all rejections based on Gauntlet be withdrawn. Nonetheless, the Patent Owner addresses Gauntlet below as though it is qualified prior art.

b) Gauntlet has not been shown to either expressly or inherently, teach each and every element of independent claims 1, 17, and 33.

- (1) Gauntlet has not been shown to teach "a secure domain name" and "a secure domain name service".

Gauntlet has not been shown to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Gauntlet is an administrator's guide describing the use and operation of firewall software. According to Gauntlet, "[a] firewall is a single point of defense that protects one side from the other. In networking situations, this

Control Number: 95/001,270

usually means protecting a company's private network from other networks to which it is connected." Gauntlet at 1-1; Nieh Dec. at ¶ 52. Gauntlet teaches a system that prohibits all network traffic through the firewall unless it is "expressly permitted." Gauntlet at 1-1; Nieh Dec. at ¶ 52.

The disclosed firewall operates as follows. The firewall necessarily must see the network traffic communicating with the protected side of the wall, *i.e.*, the private network. Gauntlet at 1-6; Nieh Dec. at ¶ 53. After receiving a packet, the firewall checks the source and destination address of the packet against its user-defined rules, and then checks the type of request sought. Gauntlet at 1-8; Nieh Dec. at ¶ 53. If the requested service is supported and authorized, the appropriate program is called and the request is processed. Gauntlet at 1-8; Nieh Dec. at ¶ 53.

When determining if access should be permitted or denied, the firewall checks the IP address provided in the packet request against the user-provided rules. Gauntlet at 5-1; Nieh Dec. at ¶ 54. The rules can be defined by hostname or by IP address. Gauntlet at 5-1; Nieh Dec. at ¶ 54. Because the received packet identifies sources and destinations by IP addresses, if the rule is defined by hostname, additional steps are taken to convert an IP address identified in the packet to a hostname. Gauntlet at 5-2; Nieh Dec. at ¶ 54. In other words, "the proxy must use DNS to map the source or destination address (in the packet) into a host name" – the proxy performs a reverse DNS lookup. Gauntlet at 5-2; Nieh Dec. at ¶ 54.

The Gauntlet firewall also offers Point-to-Point Tunneling Protocol ("PPTP") services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. Gauntlet at 18-1; Nieh Dec. at ¶ 55. To allow PPTP connections, however, the administrator of the firewall "must advertise the IP address of the PPTP server" and users "must connect directly to the server IP address." Gauntlet at 18-1; Nieh Dec. at ¶ 55. To "advertise" an IP address, as used in Gauntlet, merely requires that the IP address be accessible to the public. Nieh Dec. at ¶ 55.

Gauntlet has not been shown to describe or suggest a secure domain name as recited in claims 1, 17, and 33. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a secure domain name. *See* Request at 42; Nieh Dec. at ¶ 56. For the reasons stated at the outset of Section I.C., a secure domain name cannot be properly read to be a domain name that just

Control Number: 95/001,270

happens to be associated with a server which is used to establish PPTP connections between a client and a target. Nieh Dec. at ¶ 56.

Similarly, to the extent that Gauntlet describes a conventional DNS, a secure domain name service cannot be properly read to be a conventional DNS. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a secure domain name, and the resolution of that domain name into a network address occurs at a secure domain name service. Request at 42; Nieh Dec. at ¶ 57. First, Gauntlet discloses the administrator of the firewall “must advertise the IP address of the PPTP server” and users “must connect directly to the server IP address.” Gauntlet at 18-1; Nieh Dec. at ¶ 57. Gauntlet has not been shown to disclose a DNS resolution for a hostname for a PPTP server. Nieh Dec. at ¶ 57. Second, to the extent that Gauntlet describes a DNS, it describes a conventional DNS and not a secure DNS. Nieh Dec. at ¶ 57. As noted at the outset of Section I.C., a secure domain name service differs from a conventional DNS. Nieh Dec. at ¶ 57.

For at least these reason, Gauntlet fails to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33 and dependent claims 10, 12-15, 26, and 28-31.

(2) Gauntlet fails to teach “receiving from the secure domain name service a response message containing the secure computer network address.”

The Request alleges that the use of a PPTP service, offered by the Gauntlet firewall software, requires the use of a PPTP server whose network address is a secure computer network address. Nieh Dec. at ¶ 58. The Gauntlet firewall offers PPTP services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. Nieh Dec. at ¶ 58; Gauntlet at 18-1.

As outlined at the outset of Section I.C., the network address of a PPTP server is not a secure computer network address because it does not require authorization for access. Nieh Dec. at ¶¶ 11, 58. That is, a client can communicate with the PPTP server without authorization. *Id.*

For at least these reasons, Gauntlet fails to teach a secure computer network address, as recited in claims 1, 17, and 33. Therefore, the Patent Owner respectfully requests

Control Number: 95/001,270

reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

7. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 103(a) in View of “Microsoft Windows NT Technical Support Hands-on, Self-Paced Training for Supporting Version 4.0” (hereafter “Hands-On”) in view of “Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers” (hereafter “Installing NT”).

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hands-On in view of Installing NT. The rejection is based on the reasons given on pages 45-52 and Appendix G of the Request. The Patent Owner respectfully traverses this rejection because (i) Installing NT has not been shown to be prior art under § 103(a) and (ii) even if, for the sake of argument, Installing NT qualifies as prior art, Installing NT and Hands-On, alone or in combination, are not seen to show either expressly or inherently, each and every element of each of the independent claims 1, 17, and 33.

a) Installing NT has not been shown to be prior art.

Both the Office Action and the Request assert that Installing NT was published in 1997 without any stated support. Request at 6; Office Action at 3. The Patent Owner can only presume that this assertion arises from the copyright date range printed on the face of the reference. *See* Installing NT at *iii*. As stated in Section I.B.3., above, this copyright date range is not the publication date of Installing NT and the Office Action has failed to make any showing that it is. Further, the document, on its face, designates itself as a “White Paper.” Installing NT at cover page.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Installing NT is prior art and requests all rejections based on Installing NT be withdrawn. Nonetheless, the Patent Owner addresses Installing NT below as though it is qualified prior art.

b) Hands-On and Installing NT do not either expressly or inherently, teach each and every element of independent claims 1, 17, and 33.

(1) Hands-On and Installing NT fail to teach a “secure domain name” or a “secure domain name service.”

Installing NT is a white paper on the PPTP network protocol. See Installing NT at 1; Nieh Dec. at ¶ 59. Installing NT discloses the creation of a phonebook entry to dial a PPTP server. Installing NT at 20-22; Nieh Dec. at ¶ 59. The Request refers to Figure 12 in Installing NT to disclose a domain name for a PPTP server; Figure 12 is reproduced below. Nieh Dec. at ¶ 59. The Request, at page 47, refers to this figure to state that “PPTP connections can be identified using domain names” by indicating that the “Entry name” in the Figure is the domain name. *Id.* This is incorrect. *Id.* The “Entry name” is simply an arbitrary name to identify the Phonebook entry. *Id.* It does not *correspond* to a domain name of a PPTP server that would be resolved via a “traditional DNS server” to the network address of the PPTP server, as asserted on page 48 of the Request. *Id.*

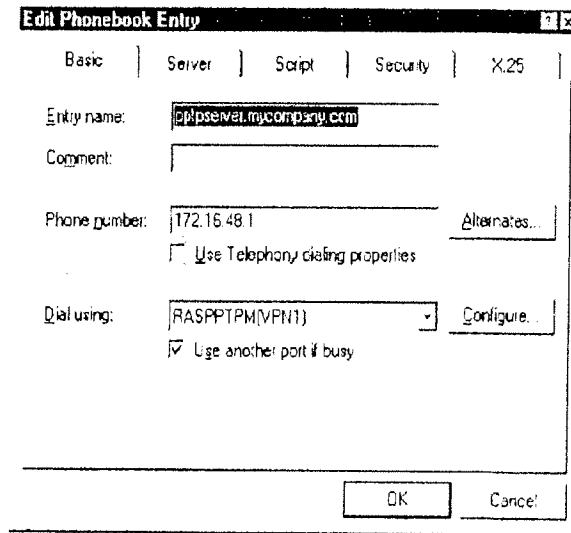


Figure 12 - Example Phonebook entry for PPTP server and a VPN device

Hands-On is a technical and training manual for Microsoft Windows NT. The Request describes Hands-On as disclosing PPTP, traditional DNS according to RFC 1035, and an AutoDial feature, which is described below. Request at 45-51; Nieh Dec. at ¶ 60.

Hands-On and Installing NT, either alone or in the proposed combination, fail to describe or suggest a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33. The Request alleges that Installing NT teaches that a name for a PPTP server is a

Control Number: 95/001,270

“secure domain name.” Nieh Dec. at ¶ 61; Request at 47. The Request asserts that, a PPTP server’s network address is a secure network address and that identifying the PPTP server with a domain name teaches a “secure domain name.” Nieh Dec. at ¶ 61. To the contrary, such an arbitrary identification is not a secure domain name. Nieh Dec. at ¶ 61. For the reasons stated above at the outset of Section I.C., a secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and a target. Nieh Dec. at ¶ 61. Neither the Office Action nor the Request demonstrate any aspect of Installing NT teaching anything other than a domain name that just happens to be associated with a PPTP server. Nieh Dec. at ¶ 61.

Hands-On similarly has not been shown to describe this feature. Nieh Dec. at ¶ 62. Notably, the Request does not rely on this reference to show this feature. As such, the Patent Owner does not believe that the proposed addition of subject matter from this reference remedies the shortcomings of Installing NT to describe or suggest a secure domain name. Nevertheless, for the reasons stated in Section I.C., to the extent that Hands-On discloses domain names, such a disclosure does not teach a secure domain name as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 62.

The Request also alleges that Hands-On discloses a secure domain name service. Request at 48-49; Nieh Dec. at ¶ 63. The Request asserts that Hands-On discloses two “lookup services” that allegedly disclose the secure domain name service recited in claim 1, 17, and 33. Request at 48; Nieh Dec. at ¶ 63. The first one is a “traditional DNS server.” Request at 48; Nieh Dec. at ¶ 63. According to the Request, sending a query message to a traditional DNS to resolve the domain name of the PPTP server disclosed in Installing NT (and described above) renders the traditional DNS a secure domain name service. Request at 48; Nieh Dec. at ¶ 63. For the reasons stated at the outset of Section I.C., a conventional DNS system is not transformed into a secure domain name service by merely resolving a query, that, unbeknownst to the secure domain name service, is requesting the address of a PPTP server.

The second “look-up service” disclosed in Hands-On also does not disclose the secure domain name service of claims 1, 17, and 33. Request at 48; Nieh Dec. at ¶ 64. This “alternative ‘lookup service’” is called AutoDial. Nieh Dec. at ¶ 64; Request at 48. AutoDial “maps and maintains network addresses to phonebook entries” such that, when an application or command requests access to an IP address, the client computer will match that network address

Control Number: 95/001,270

to the phonebook entry and dial the phone number associated with that network address. Hands-On at 462; Nieh Dec. at ¶ 64. Although an AutoDial database can include IP addresses and Internet host names, these addresses are each associated with a phonebook entry, which provides a phone number to be dialed for connecting with said IP addresses and Internet host names. Nieh Dec. at ¶ 64. Thus, AutoDial is not disclosed to resolve domain names to IP addresses, much less to resolve a secure domain name into a secure computer network address. Nieh Dec. at ¶ 64. Nevertheless, even assuming for the sake of argument that AutoDial were shown to teach a conventional DNS, a conventional DNS does not teach a secure domain name service for the reasons stated above at the outset of Section I.C. Nieh Dec. at ¶ 64.

As such, this alternative implementation also fails to describe or suggest a secure domain name service as recited in claim 1, 17, and 33. Therefore, the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of independent claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

(2) Hands-On and Installing NT fail to describe or suggest receiving from a secure domain name service a secure computer network address

The Request alleges that, because a PPTP server, which enables a PPTP connection between a client and a target, may be referenced by a domain name, its domain name is a “secure domain name” and its network address is a “secure computer network address.” Request at 47; Nieh Dec. at ¶ 65. The network address for a PPTP server is not a secure network address because a client can communicate with it without authorization, as stated above at the outset of Section I.C. Nieh Dec. at ¶¶ 65, 11.

As such, the cited documents have not been shown to describe or suggest “receiving from a secure domain name service a secure computer network address,” as recited in claims 1, 17, and 33. Accordingly, the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

c) Secondary Considerations of Non-Obviousness

For the reasons stated in Section I.C.2.c above, it would not have been obvious to combine Hands-On and Installing NT in the manner proposed in the Office Action. Therefore,

Control Number: 95/001,270

the Patent Owner respectfully requests reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26, and 28-31.

8. The Rejection of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 Under 35 U.S.C. § 102(a) in View of “Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources” (hereafter “Microsoft VPN”)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the ‘180 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Microsoft VPN. The rejection is based on the reasons given on pages 52-56 and Appendix H of the Request. The Patent Owner respectfully traverses this rejection because (i) Microsoft VPN has not been shown to be prior art under § 102(a) and (ii) even if, for the sake of argument, Microsoft VPN qualifies as prior art, Microsoft VPN has not been shown to either expressly or inherently, teach each and every element of each independent claim 1, 17, and 33.

a) Microsoft VPN has not been shown to be prior art under §102(a).

Both the Office Action and the Request assert that Microsoft VPN was published in on January 1, 2000, without any stated support. Request at 6; Office Action at 3. The Patent Owner can only presume that this assertion arises from the date printed on the face of the reference. *See* Microsoft VPN at cover page. As stated in Section I.B.3., above, this copyright date range is not the publication date of Microsoft VPN and the Office Action has failed to make any showing that it is.

Further, the closeness of proximity of the alleged publication date of Microsoft VPN to the April 26, 2000 priority date of the ‘180 Patent makes the availability of this reference as prior art even more dubious. Suppose the relied upon sections of the Microsoft VPN were actually created on “January 1, 2000.” Under these circumstances, it is possible that the document, although created, was not disseminated until after the priority date of the ‘180 Patent, four months after creation. Under these circumstances, Microsoft VPN clearly would not be eligible to be relied upon as prior art to the ‘180 Patent.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Microsoft VPN is prior art and requests all rejections based on Microsoft VPN be

Control Number: 95/001,270

withdrawn. Nonetheless, the Patent Owner addresses Microsoft VPN below as though it is qualified prior art.

b) Microsoft VPN has not been shown to either expressly or inherently, teach each and every element of independent claims 1, 17, and 33.

(1) Microsoft VPN fails to teach a “secure domain name” or “secure domain name service.”

Microsoft VPN is a compilation of various Microsoft documents. As identified by the Request, Microsoft VPN discloses PPTP connections for remote users to access a corporate network. Request at 52; Nieh Dec. at ¶ 66. Microsoft VPN discloses creating an IP address or host name of a corporate office “VPN” server. Microsoft VPN at 32; Nieh Dec. at ¶ 66. Microsoft VPN also discloses a conventional DNS structure. Microsoft VPN at 64-66; Nieh Dec. at ¶ 66. Microsoft VPN, however, has not been shown to teach a secure domain name or secure domain name service, as recited in claims 1, 17, and 33. Nieh Dec. at ¶ 66.

The Request asserts that the hostname associated with a PPTP server, which is used to establish PPTP connections between a client and a target computer is a “secure domain name.” Request at 54; Nieh Dec. at ¶ 67. A secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and target for the reasons stated at the outset of Section I.C., above. Nieh Dec. at ¶ 67.

The Request also alleges that, since Microsoft VPN discloses a conventional DNS, which resolves domain names, a DNS request for the IP address for a PPTP server renders the traditional DNS a secure domain name service. Request at 54; Nieh Dec. at ¶ 68. This is incorrect. A conventional DNS is not transformed into a secure domain name service merely by resolving a request for the IP address of a server which is used to establish PPTP connections. Nieh Dec. at ¶ 68. As stated at the outset of Section I.C., above, disclosure of a conventional DNS does not disclose a secure domain name service. Nieh Dec. at ¶ 68. Accordingly, because Microsoft VPN does not describe or suggest a secure domain name or a secure domain name service as recited in claims 1, 17, and 33, the Patent Owner respectfully requests that reconsideration and withdrawal of the rejections of claims 1, 17, and 33, and dependent claims 10, 12-15, 26 and 28-31.

Control Number: 95/001,270

(2) Microsoft VPN fails to teach receiving from a secure domain name service a computer network address.

The Request alleges that the network address of a PPTP server, which enables a PPTP connection between a client and a target, is a "secure computer network address." Request at 54; Nieh Dec. at ¶ 69. The network address for a PPTP server is not a secure network address because a client can communicate with it without authorization, as stated above at the outset of Section I.C. Nieh Dec. at ¶¶ 69, 11.

Accordingly, because Microsoft VPN does not teach "a secure computer network address," the Patent Owner respectfully requests reconsideration and withdrawal of the rejection of claims 1, 17, and 33 and dependent claims 10, 12-15, 26, and 28-31.

II. Conclusion

For at least the reasons set forth above, the rejection of claims 1, 10, 12-15, 17, 26, 28-31, and 33 should be withdrawn. Reconsideration and prompt confirmation of claims 1, 10, 12-15, 17, 26, 28-31, and 33 are respectfully requested.

Please charge our Deposit Account No. 501133 any fees or credit any overcharges relating to this Response.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/

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

Matthew E. Leno, Reg. No. 41,149

Hasan M. Rashid, Reg. No. 62,390

McDermott Will & Emery LLP

Attorneys for Patent Owner

28 State Street
Boston, MA 02109-1775
Phone: 617.535.4000
Facsimile: 617.535.3800
Date: April 19, 2010

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
Victor Larson, et al.)
)
U.S. Patent No.: 7,188,180)
Filed: November 7, 2003) Examiner:
Issued: March 6, 2007) Andrew L. Nalven
)
For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
SECURE COMMUNICATION LINK)
BETWEEN COMPUTERS OF)
VIRTUAL PRIVATE NETWORK)
)
Reexamination Proceeding)
Control No.: 95/001,270)
Filed: December 8, 2009)

NOTICE OF CONCURRENT PROCEEDINGS UNDER 37 C.F.R. § 1.985

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. § 1.985 and MPEP § 2686, Patent Owner, VirnetX, Inc. (“VirnetX”) provides this Notification to the Office.

Patent Owner, VirnetX, Inc., and Microsoft have settled their concurrent litigation proceedings (*VirnetX, Inc. v. Microsoft Corp.*, Case Nos. 6:07-cv-00080-LED, 6:10-cv-00094 (E.D. Tex.)) involving the patent at issue in this *inter partes* reexamination proceeding.

A Stipulation of Dismissal was filed in each of the above-referenced litigations on May 18, 2010, attached hereto as Exhibits A and B.

Control Number: 95/001,270

The commissioner is hereby authorized to charge any fees required 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, P.C., Reg. No. 26,418

Matthew E. Leno, Reg. No. 41,149

Hasan M. Rashid, Reg. No. 62,390

McDermott Will & Emery LLP

Attorneys for Patent Owner

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com
mleno@mwe.com
hrashid@mwe.com
Date: May 24, 2010

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:)
Victor Larson, et al.)
))
U.S. Patent No.: 7,188,180)
Filed: November 7, 2003) Examiner:
Issued: March 6, 2007) Andrew L. Nalven
))
For: METHOD FOR ESTABLISHING) Group Art Unit: 3992
SECURE COMMUNICATION LINK)
BETWEEN COMPUTERS OF VIRTUAL)
PRIVATE NETWORK)
))
Reexamination Proceeding)
Control No.: 95/001,270)
Filed: December 8, 2009)

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that a re-filing of the Response originally filed with the United States Patent and Trademark Office on April 19, 2010, a Notice of Resubmission, a Notice of Concurrent Proceedings Under 37 C.F.R. § 1.985 and a Petition Under 37 C.F.R. § 1.183 to Waive 37 C.F.R. § 1.955, all filed with the United States Patent and Trademark Office on May 24, 2010 were served this 24th day of May, 2010 on Requester by causing a true copy of same by first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Patent Owner
**Please recognize our Customer No. 23630 as
our correspondence address.**

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: May 24, 2010

Electronic Patent Application Fee Transmittal

Application Number:	95001270
Filing Date:	08-Dec-2009
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	077580-0090

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Petition fee- 37 CFR 1.17(f) (Group I)	1462	1	400	400

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				400

Electronic Acknowledgement Receipt

EFS ID:	7677899
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	24-MAY-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:37:17
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$400
RAM confirmation Number	9116
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)

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	Reexam Miscellaneous Incoming Letter	Notice_Resubmission90.pdf	23459	no	1
			0d15f689f4596595e688322bf75521f47b738044		
Warnings:					
Information:					
2	Response after non-final action-owner timely	Response90.pdf	1767741	no	34
			8d76af625592c0596e41d48f252c844a78f7315		
Warnings:					
Information:					
3	Notice of concurrent proceeding(s)	Notice_Concurrent_Proceedings90.pdf	226423	no	11
			3d9331cf724779533d201b9510a2db671e8aff5d		
Warnings:					
Information:					
4	Reexam Miscellaneous Incoming Letter	Petition_Waive90.pdf	45321	no	2
			f88ed0edcebbcd023fae2720e37dca08325c1c9d3		
Warnings:					
Information:					
5	Reexam Certificate of Service	CertServ90.pdf	27603	no	1
			889146aa7f3b34c7f57a31a862dfce3fd22c843c		
Warnings:					
Information:					
6	Fee Worksheet (PTO-875)	fee-info.pdf	30500	no	2
			9d4fe50faa02335f5756d862c34a2b8a87105106		
Warnings:					
Information:					
Total Files Size (in bytes):			2121047		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
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	

3992

MAIL DATE	DELIVERY MODE
06/16/2010	PAPER

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 conventional 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 convention 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

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.	

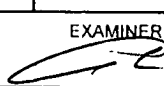
U.S. PATENT APPLICATION PUBLICATIONS

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 (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	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				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.)

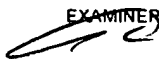
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
AW	C998	Microsoft 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

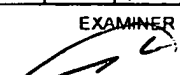
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant 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.)

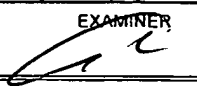
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	C1026	Microsoft 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.mspxpftrue). (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	

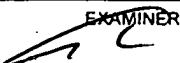

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

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

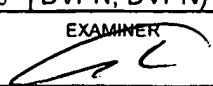
Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	9	of	19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

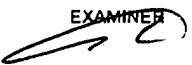
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
AN	C1074	H. Schulzrinne, "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</i> <draft-eitf-cat-krb-dns-locate-oo.txt> (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 <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	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	<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)			
	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.aspx (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.aspx (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.aspx (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/ras40/rrasch01.aspx (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.aspx (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 SSH2.0 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 6/2/00

*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: 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)
	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 15 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 <i>(Use as many sheets as necessary)</i>				Application Number	95/001,270
				Filing Date	December 8,2009
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Andrew L. Nalven
				Docket Number	077580-0090

CERTIFICATION STATEMENT

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

Information Disclosure Statement is being filed after the receipt of an office action.

Under 37 C.F.R. 1.98(a)(2)(ii), copies of U.S. Patents and patent application publications are not required. Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies at the Examiner's request.

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

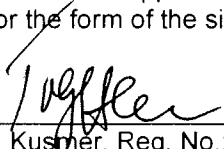
The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of \$180.00, or further fees which may be due, to Deposit Account 50-1133.

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.



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

Date: *6-25-10*

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)				ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270	
				APPLICANT Victor Larson		
				FILING DATE December 8, 2009	GROUP 3992	
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
	A100	US	4,933,846	6/12/1990	Humphrey et al.	
	A101	US	4,988,990	1/29/1991	Warrior	
	A102	US	5,276,735	1/4/1994	Boebert et al	
	A103	US	5,329,521	7/12/1994	Walsh et al.	
	A104	US	5,341,426	8/23/1994	Barney et al.	
	A105	US	5,367,643	11/22/1994	Chang et al	
	A106	US	5,559,883	9/24/1996	Williams	
	A107	US	5,561,669	10/1/1996	Lenney et al	
	A108	US	5,588,060	12/24/1996	Aziz	
	A109	US	5,625,626	4/29/1997	Umekita	
	A110	US	5,654,695	8/5/1997	Olnowich et al	
	A111	US	5,682,480	10/28/1997	Nakagawa	
	A112	US	5,689,566	11/18/1997	Nguyen	
	A113	US	5,740,375	4/14/1998	Dunne et al.	
	A114	US	5,774,660	6/30/1998	Brendel et al	
	A115	US	5,787,172	7/28/1998	Arnold	
	A116	US	5,796,942	8/18/1998	Esbensen	
	A117	US	5,805,801	9/8/1998	Holloway et al.	
	A118	US	5,842,040	11/24/1998	Hughes et al.	
	A119	US	5,845,091	12/1/1998	Dunne et al.	
	A120	US	5,867,650	2/2/1998	Osterman	
	A121	US	5,870,610	2/9/1999	Beyda et al.	
	A122	US	5,878,231	5/2/1999	Baehr et al	
	A123	US	5,892,903	4/6/1999	Klaus	
	A124	US	5,905,859	5/18/1999	Holloway et al.	
	A125	US	5,918,019	6/29/1999	Valencia	
	A126	US	5,996,016	11/30/1999	Thalheimer et al.	
	A127	US	6,006,259	12/21/1999	Adelman et al.	
	A128	US	6,006,272	12/21/1999	Aravamudan et al	
	A129	US	6,016,318	1/18/2000	Tomoike	
	A130	US	6,016,512	1/18/2000	Huitema	
	A131	US	6,041,342	3/21/2000	Yamaguchi	
	A132	US	6,061,736	5/9/2000	Rochberger et al	
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.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)				ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270	
				APPLICANT Victor Larson		
				FILING DATE December 8, 2009	GROUP 3992	
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
	A133	US	6,092,200	7/18/2000	Muniyappa et al.	
	A134	US	6,119,234	9/12/2000	Aziz et al.	
	A135	US	6,147,976	11/14/2000	Shand et al.	
	A136	US	6,157,957	12/5/2000	Berthaud	
	A137	US	6,158,011	12/5/2000	Chen et al.	
	A138	US	6,168,409	1/2/2001	Fare	
	A139	US	6,175,867	1/16/2001	Taghadoss	
	A140	US	6,178,409	1/23/2001	Weber et al.	
	A141	US	6,178,505	1/23/2001	Schneider et al	
	A142	US	6,179,102	1/30/2001	Weber, et al.	
	A143	US	6,222,842	4/24/2001	Sasyan et al.	
	A144	US	6,233,618	5/15/2001	Shannon	
	A145	US	6,243,360	6/5/2001	Basilico	
	A146	US	6,243,749	6/5/2001	Sitaraman et al.	
	A147	US	6,243,754	6/5/2001	Guerin et al	
	A148	US	6,256,671	7/3/2001	Strentzsch et al.	
	A149	US	6,263,445	7/17/2001	Blumenau	
	A150	US	6,286,047	9/4/2001	Ramanathan et al	
	A151	US	6,301,223	10/9/2001	Hrastar et al	
	A152	US	6,308,274	10/23/2001	Swift	
	A153	US	6,311,207	10/30/2001	Mighdoll et al	
	A154	US	6,324,161	11/27/2001	Kirch	
	A155	US	6,330,562	12/11/2001	Boden et al.	
	A156	US	6,332,158	12/18/2001	Risley et al.	
	A157	US	6,353,614	3/5/2002	Borella et al.	
	A158	US	6,430,155	8/6/2002	Davie et al	
	A159	US	6,430,610	8/6/2002	Carter	
	A160	US	6,487,598	11/26/2002	Valencia	
	A161	US	6,505,232	1/7/2003	Mighdoll et al	
	A162	US	6,510,154	1/21/2003	Mayes et al	
	A163	US	6,549,516	4/15/2003	Albert et al	
	A164	US	6,571,296	5/27/2002	Dillon	
	A165	US	6,571,338	5/27/2003	Shaio et al.	
	A166	US	6,581,166	7/17/2003	Hirst et al.	
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.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)	ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270
	APPLICANT Victor Larson	
	FILING DATE December 8, 2009	GROUP 3992

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
	B100	EP 0 814 589	12/29/97	Harwood et al.			
	B101	EP 0 838 930	4/29/98	Alden et al.			
	B102	EP 0 858 189	8/12/98	Maciel et al.			
	B103	DE 199 24 575	12/2/99	Provino et al.			
	B104	GB 2 317 792	4/1/98	Miner et al.			
	B105	GB 2 334 181 A	8/11/99	Noblet			
	B106	EP 836306A1	4/15/98	Sasyan et al.			
	B107	WO 9827783 A	6/25/98	Tello et al.			
	B108	WO 00/17775	3/30/00	Miller et al.			
	B109	WO 01 50688	7/12/01	Kriens			
	B110	WO 98 55930	12/10/98	Tang			
	B111	WO 98 59470	12/30/98	Kanter et al.			
	B112	WO 98/27783	6/25/98	Tello et al.			
	B113	WO 99 38081	7/29/99	Paulsen et al.			
	B114	WO 99 48303	9/23/99	Cox et al.			

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.
		See sheet Nos. 5-6

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.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION		ATTY. DOCKET NO.	SERIAL NO
(PTO-1449)		077580-0090	95/001,270
		APPLICANT Victor Larson	
		FILING DATE December 8, 2009	GROUP 3992
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.	
	C100	Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/draft302.txt on Feb. 4, 2002, 56 pages.	
	C102	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	C103	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	C104	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	C105	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	C106	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	C107	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	C108	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	C109	Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.	
	C110	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/glossary.html on Feb. 21, 2002, 25 pages.	
	C111	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	C112	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	C113	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	C114	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	C115	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	C116	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
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.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)		ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270
		APPLICANT Victor Larson	
		FILING DATE December 8, 2009	GROUP 3992
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.	
	C117	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	C118	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	C119	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	C120	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	C121	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	C122	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	C123	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	
	C124	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	C125	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	C126	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	C127	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conferece on Communications architectures & protocols. pp. 84-91, ACM Press, NY,NY 1986.	
	C128	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	C129	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	C130	FASBENDER, A. et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	C131	156. Finding Your Way Through the VPN Maze (1999) ("PGP")	
	C132	WatchGuard Technologies, Inc., WatchGuard LiveSecurity for MSS Powerpoint (Feb. 14 2000) (resubmitted)	
	C133	WatchGuard Technologies, Inc., MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes (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.

BS199 1551744-1.068911.0140

Electronic Acknowledgement Receipt

EFS ID:	7895754
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Melissa Molchan
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	25-JUN-2010
Filing Date:	08-DEC-2009
Time Stamp:	15:29:23
Application Type:	inter partes reexam

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	077580090IDS.pdf	223026 <small>3c48e644adfa3254cab28cfe1104c97dff99d682</small>	no	7

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Total Files Size (in bytes):

223026

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.

Litigation Search Report CRU 3999

Reexam Control No. 95/001,270

TO: ANDREW NALVEN
Location: CRU
Art Unit: 3992
Date: 12/01/10

From: MANUEL SALDANA
Location: CRU 3999
MDW 7C55
Phone: (571) 272-7740

MANUEL.SALDANA@uspto.gov

Search Notes

Litigation was found for US Patent Number: **7,188,180**

DOCKET 6:10CV417 (NOT CLOSED)

DOCKET 6:10CV94 (CLOSED 05/25/10).

- 1) I performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.
- 2) I performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.
- 3) I performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.
- 4) I performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.
- 5) I performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

KEYCITE

H US PAT 7188180 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, Assignee: VimetX, Inc. (Mar 06, 2007)

History**Direct History**

H 1 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6502135, 2002 WL 31892276 (U.S. PTO Utility Dec 31, 2002) (NO. 09/504783)

Construed by

H 2 VimetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)

H 3 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK WITHOUT USER ENTERING ANY CRYPTOGRAPHIC INFORMATION, US PAT 6839759, 2005 WL 132324 (U.S. PTO Utility Jan 04, 2005) (NO. 10/702522)

Construed by

H 4 VimetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)

=> 5 **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**, US PAT 7188180, 2007 WL 665444 (U.S. PTO Utility Mar 06, 2007) (NO. 10/702486)

Construed by

H 6 VimetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)

Court Documents**Verdict and Settlement Summaries (U.S.A.)****E.D.Tex.**

7 VimetX Inc. v. Microsoft Corp., 2010 WL 1213036 (Verdict and Settlement Summary) (E.D.Tex. Mar. 16, 2010) (NO. 607-CV-80)

Trial Court Documents (U.S.A.)

E.D.Tex. Trial Pleadings

- 8 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827531 (Trial Pleading) (E.D.Tex. Apr. 5, 2007) **Plaintiff Virnetx Inc.'s First Amended Complaint for Patent Infringement** (NO. 607CV80, TJW)
- 9 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827532 (Trial Pleading) (E.D.Tex. May 4, 2007) **Microsoft's Answer, Defenses, and Counterclaims to Virnetx's First Amended Complaint** (NO. 607CV80, LED)
- 10 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827533 (Trial Pleading) (E.D.Tex. May 24, 2007) **Plaintiff Virnetx's Reply to Defendant Microsoft's Counterclaims** (NO. 607CV80, LED)
- 11 VIRNETX INC., Plaintiff, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, Involuntary plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 2775842 (Trial Pleading) (E.D.Tex. Jun. 10, 2008) **Plaintiff Virnetx Inc.'s and Science Applications International Corporation's First Amended Complaint for Patent Infringement** (NO. 607CV00080)

E.D.Tex. Expert Testimony

- 12 VIRNETX, INC., v. MICROSOFT CORPORATION., 2008 WL 7465386 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) (**Report or Affidavit of Mark T. Jones, Ph.D.**) (NO. 07CV00080)
- 13 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465387 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **Exhibit E: Summary of Opinions of Dr. David B. Johnson Regarding Claim Construction** (NO. 607-CV-80, LED)
- 14 VIRNETX, INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465388 (Partial Expert Testimony) (E.D.Tex. Dec. 17, 2008) **Oral & Videotaped Deposition of David P. Johnson, Ph.D.** (NO. 607CV80, LED)
- 15 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5631263 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 16 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465389 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 17 VIRNETX INC., Plaintiff, Science Applications International Corporation, Involuntary Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5653416 (Expert Report and Affidavit) (E.D.Tex. Dec. 30, 2008) **Declaration of Mark T. Jones, Ph.D.** (NO. 607CV80, LED)
- 18 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 423638 (Expert Report and Affidavit) (E.D.Tex. Jan. 20, 2009) **Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 19 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732176 (Expert Report and Affidavit)

- (E.D.Tex. Feb. 3, 2009) **Reply Declaration of Mark T. Jones, Ph.D** (NO. 607CV80, LED)
- 20 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732177 (Expert Report and Affidavit) (E.D.Tex. Feb. 10, 2009) **Reply Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 21 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732178 (Expert Report and Affidavit) (E.D.Tex. Dec. 18, 2009) **Declaration of Dr. Stephen Wicker in Support of Microsoft's Motion for Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607-CV-80, LED)

E.D.Tex. Trial Motions, Memoranda And Affidavits

- 22 VIRNETX INC., Plaintiff , SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, Involuntary plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5531230 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Dec. 30, 2008) **Plaintiff Virnetx Inc.'s Opening Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV00080)
- 23 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155346 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Jan. 20, 2009) **Microsoft's Responsive Claim Construction Brief** (NO. 607-CV-80, LED)
- 24 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155347 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 3, 2009) **Plaintiff Virnetx Inc.'s Reply Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV80, LED)
- 25 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155348 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 10, 2009) **Microsoft's Sur-Reply Claim Construction Brief** (NO. 607-CV-80, LED)
- 26 VIRNETX INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 4654324 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Sep. 3, 2009) **Plaintiff Virnetx Inc.'s Response to Defendant Microsoft Corporation's Motion for Clarification to Amend Appendix B to Claim Construction Opinion** (NO. 607CV80(LED))
- 27 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5819696 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Dec. 18, 2009) **Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607CV00080)

E.D.Tex.

- 28 Mark T. Jones, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914105 (Court-filed Expert Resume).(E.D.Tex. 2007) **Expert Resume of Mark T. Jones** (NO. 07CV00080)
- 29 David B. Johnson, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007

WL 6914106 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of David B. Johnson** (NO. 07CV00080)

E.D.Tex. Trial Filings

- 30 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827534 (Trial Filing) (E.D.Tex. Aug. 29, 2007) **Joint Conference Report** (NO. 607CV80, LED)
- 31 VIRNETX INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5356442 (Trial Filing) (E.D.Tex. Oct. 31, 2008) **Joint Claim Construction and Prehearing Statement** (NO. 607CV80, LED)

E.D.Tex. Verdicts, Agreements and Settlements

- 32 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2010 WL 1046839 (Verdict, Agreement and Settlement) (E.D.Tex. Jan. 14, 2010) **Stipulation of Dismissal** (NO. 607-CV-80, LED)
- 33 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2010 WL 1046840 (Verdict, Agreement and Settlement) (E.D.Tex. Jan. 14, 2010) **Joint Stipulation Regarding Microsoft's Inequitable Conduct Counterclaims and Affirmative Defenses** (NO. 607-CV-80, LED)

Dockets (U.S.A.)

E.D.Tex.

- 34 VIRNETX, INC. v. MICROSOFT CORPORATION, NO. 6:07cv00080 (Docket) (E.D.Tex. Feb. 15, 2007)

Expert Court Documents (U.S.A.)

E.D.Tex.

- 35 VirnetX Inc. v. Microsoft Corp., 2010 WL 1213036 (Verdict and Settlement Summary) (E.D.Tex. Mar. 16, 2010) (NO. 607-CV-80)

E.D.Tex. Expert Testimony

- 36 VIRNETX, INC., v. MICROSOFT CORPORATION., 2008 WL 7465386 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) (**Report or Affidavit of Mark T. Jones, Ph.D.**) (NO. 07CV00080)
- 37 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465387 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **Exhibit E: Summary of Opinions of Dr. David B. Johnson Regarding Claim Construction** (NO. 607-CV-80, LED)
- 38 VIRNETX, INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465388 (Partial Expert Testimony) (E.D.Tex. Dec. 17, 2008) **Oral & Videotaped Deposition of David**

- P. Johnson, Ph.D.** (NO. 607CV80, LED)
- 39 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5631263 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) **(Partial Testimony of Mark T. Jones, Ph.D.)** (NO. 607-CV-80, LED)
- 40 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465389 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) **(Partial Testimony of Mark T. Jones, Ph.D.)** (NO. 607-CV-80, LED)
- 41 VIRNETX INC., Plaintiff, Science Applications International Corporation, Involuntary Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5653416 (Expert Report and Affidavit) (E.D.Tex. Dec. 30, 2008) **Declaration of Mark T. Jones, Ph.D.** (NO. 607CV80, LED)
- 42 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 423638 (Expert Report and Affidavit) (E.D.Tex. Jan. 20, 2009) **Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 43 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732176 (Expert Report and Affidavit) (E.D.Tex. Feb. 3, 2009) **Reply Declaration of Mark T. Jones, Ph.D** (NO. 607CV80, LED)
- 44 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732177 (Expert Report and Affidavit) (E.D.Tex. Feb. 10, 2009) **Reply Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 45 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732178 (Expert Report and Affidavit) (E.D.Tex. Dec. 18, 2009) **Declaration of Dr. Stephen Wicker in Support of Microsoft's Motion for Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607-CV-80, LED)

E.D.Tex.

- 46 Mark T. Jones, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914105 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of Mark T. Jones** (NO. 07CV00080)
- 47 David B. Johnson, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914106 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of David B. Johnson** (NO. 07CV00080)

Patent Family

- 48 INFORMATION TRANSMISSION INVOLVES COMPARING DISCRIMINATOR VALUE FOR EACH RECEIVED DATA PACKET WITH SET OF VALID DISCRIMINATOR VALUES, ACCEPTING RECEIVED DATA PACKET FOR FURTHER PROCESSING WHILE DETECTING MATCH, Derwent World Patents Legal 2000-399393

Assignments

- 49 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DE-

TAILS). Number of Pages: 005, (DATE RECORDED: Jan 10, 2007)
50 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DE-
TAILS). Number of Pages: 003, (DATE RECORDED: Nov 07, 2003)

Patent Status Files

- .. Request for Re-Examination, (OG DATE: Mar 02, 2010)
- .. Certificate of Correction, (OG DATE: Aug 28, 2007)

Docket Summaries

- 53 VIRNETX INC. v. CISCO SYSTEMS, INC. ET AL, (E.D.TEX. Aug 11, 2010) (NO. 6:10CV00417), (35 USC 271 PATENT INFRINGEMENT)
- 54 VIRNETX INC. v. MICROSOFT CORPORATION, (E.D.TEX. Mar 17, 2010) (NO. 6:10CV00094), (35 USC 271 PATENT INFRINGEMENT)

Litigation Alert

- 55 Derwent LitAlert P2010-35-19 (Aug 11, 2010) Action Taken: complaint for PATENT INFRINGEMENT
- 56 Derwent LitAlert P2010-13-31 (Mar 17, 2010) Action Taken: complaint

Prior Art (Coverage Begins 1976)

- C** 57 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 7010604Assignee: Science Applications International, (U.S. PTO Utility 2006)
- H** 58 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6502135Assignee: Science Applications International, (U.S. PTO Utility 2002)
- C** 59 APPARATUS AND METHOD FOR ESTABLISHING A CRYPTOGRAPHIC LINK BETWEEN ELEMENTS OF A SYSTEM, US PAT 5787172Assignee: The Merdan Group, Inc., (U.S. PTO Utility 1998)
- C** 60 AUTOCONFIGURABLE METHOD AND SYSTEM HAVING AUTOMATED DOWNLOADING, US PAT 5870610Assignee: Siemens Business Communication Systems,, (U.S. PTO Utility 1999)
- C** 61 CRYPTOGRAPHIC KEY MANAGEMENT APPARATUS AND METHOD, US PAT 5341426Assignee: Motorola, Inc., (U.S. PTO Utility 1994)
- C** 62 DOMAIN NAME ROUTING, US PAT 6119171Assignee: IP Dynamics, Inc., (U.S. PTO Utility 2000)
- C** 63 DOMAIN NAME SYSTEM LOOKUP ALLOWING INTELLIGENT CORRECTION OF SEARCHES AND PRESENTATION OF AUXILIARY INFORMATION, US PAT 6332158 (U.S. PTO Utility 2001)
- C** 64 DYNAMIC NETWORK ADDRESS UPDATING, US PAT 6243749Assignee: Cisco Techno-

- logy, Inc., (U.S. PTO Utility 2001)
- C** 65 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 6052788 Assignee: Network Engineering Software, Inc., (U.S. PTO Utility 2000)
 - C** 66 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 5898830 Assignee: Network Engineering Software, (U.S. PTO Utility 1999)
 - C** 67 MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS, US PAT 5905859 Assignee: International Business Machines, (U.S. PTO Utility 1999)
 - C** 68 METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION, US PAT 5796942 Assignee: Computer Associates International, Inc., (U.S. PTO Utility 1998)
 - C** 69 METHOD AND APPARATUS FOR CLIENT-HOST COMMUNICATION OVER A COMPUTER NETWORK, US PAT 6119234 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 2000)
 - C** 70 METHOD AND APPARATUS FOR CONFIGURING A VIRTUAL PRIVATE NETWORK, US PAT 6226751 Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2001)
 - C** 71 METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM, US PAT 5892903 Assignee: Internet Security Systems, Inc., (U.S. PTO Utility 1999)
 - C** 72 METHOD AND APPARATUS FOR AN INTERNET PROTOCOL (IP) NETWORK CLUSTERING SYSTEM, US PAT 6006259 Assignee: Network Alchemy, Inc., (U.S. PTO Utility 1999)
 - C** 73 METHOD AND APPARATUS FOR A KEY-MANAGEMENT SCHEME FOR INTERNET PROTOCOLS, US PAT 5588060 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1996)
 - C** 74 METHOD AND APPARATUS FOR MANAGING A VIRTUAL PRIVATE NETWORK, US PAT 6079020 Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2000)
 - C** 75 METHOD AND APPARATUS FOR PROVIDING NETWORK ACCESS CONTROL USING A DOMAIN NAME SYSTEM, US PAT 6256671 Assignee: Nortel Networks Limited, (U.S. PTO Utility 2001)
 - C** 76 METHOD AND APPARATUS FOR PROVIDING A VIRTUAL PRIVATE NETWORK, US PAT 6092200 Assignee: Novell, Inc., (U.S. PTO Utility 2000)
 - C** 77 METHOD AND PROTOCOL FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION, US PAT 6353614 Assignee: 3Com Corporation, (U.S. PTO Utility 2002)
 - C** 78 METHOD AND SYSTEM FOR AUTOMATIC DISCOVERY OF NETWORK SERVICES, US PAT 6286047 Assignee: Hewlett-Packard Company, (U.S. PTO Utility 2001)
 - C** 79 MULTI-ACCESS VIRTUAL PRIVATE NETWORK, US PAT 6158011 Assignee: V-One Corporation, (U.S. PTO Utility 2000)
 - C** 80 NETWORK COMMUNICATIONS ADAPTER WITH DUAL INTERLEAVED MEMORY BANKS SERVICING MULTIPLE PROCESSORS, US PAT 4933846 Assignee: Network Systems Corporation, (U.S. PTO Utility 1990)
 - C** 81 NETWORK WITH SECURE COMMUNICATIONS SESSIONS, US PAT 5689566 (U.S. PTO Utility 1997)

- H** 82 POLICY CACHING METHOD AND APPARATUS FOR USE IN A COMMUNICATION DEVICE BASED ON CONTENTS OF ONE DATA UNIT IN A SUBSET OF RELATED DATA UNITS, US PAT 5842040 Assignee: Storage Technology Corporation, (U.S. PTO Utility 1998)
- C** 83 SECURE DELIVERY OF INFORMATION IN A NETWORK, US PAT 6178505 Assignee: Internet Dynamics, Inc., (U.S. PTO Utility 2001)
- C** 84 SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY, US PAT 5805801 Assignee: International Business Machines, (U.S. PTO Utility 1998)
- C** 85 SYSTEM AND METHOD FOR MANAGING SECURITY OBJECTS, US PAT 6330562 Assignee: International Business Machines, (U.S. PTO Utility 2001)
- C** 86 SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE, US PAT 5878231 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1999)
- C** 87 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR MULTIPLE-ENTRY POINT VIRTUAL POINT OF SALE ARCHITECTURE, US PAT 6178409 Assignee: VeriFone, Inc., (U.S. PTO Utility 2001)
- C** 88 VIRTUAL PRIVATE NETWORK SYSTEM OVER PUBLIC MOBILE DATA NETWORK AND VIRTUAL LAN, US PAT 6016318 Assignee: NEC Corporation, (U.S. PTO Utility 2000)

Westlaw Delivery Summary Report for SALDANA,MANUEL

Date/Time of Request:	Wednesday, December 1, 2010 10:16 Central
Client Identifier:	5982987MKZC
Database:	KEYCITE-HIST
Citation Text:	US PAT 7188180
Service:	KeyCite
Lines:	486
Documents:	1
Images:	0

The material accompanying this summary is subject to copyright. Usage is governed by contract with Thomson Reuters, West and their affiliates.

KEYCITE

H US PAT 7188180 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, Assignee: VimetX, Inc. (Mar 06, 2007)

History

Direct History

H 1 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6502135, 2002 WL 31892276 (U.S. PTO Utility Dec 31, 2002) (NO. 09/504783)

Construed by

H 2 VirnetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)

H 3 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK WITHOUT USER ENTERING ANY CRYPTOGRAPHIC INFORMATION, US PAT 6839759, 2005 WL 132324 (U.S. PTO Utility Jan 04, 2005) (NO. 10/702522)

Construed by

H 4 VirnetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)

=> **5 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, US PAT 7188180, 2007 WL 665444 (U.S. PTO Utility Mar 06, 2007) (NO. 10/702486)**

Construed by

H 6 VirnetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)

Court Documents

Verdict and Settlement Summaries (U.S.A.)

E.D.Tex.

7 VirnetX Inc. v. Microsoft Corp., 2010 WL 1213036 (Verdict and Settlement Summary) (E.D.Tex. Mar. 16, 2010) (NO. 607-CV-80)

Trial Court Documents (U.S.A.)

E.D.Tex. Trial Pleadings

- 8 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827531 (Trial Pleading) (E.D.Tex. Apr. 5, 2007) **Plaintiff Virnetx Inc.'s First Amended Complaint for Patent Infringement** (NO. 607CV80, TJW)
- 9 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827532 (Trial Pleading) (E.D.Tex. May 4, 2007) **Microsoft's Answer, Defenses, and Counterclaims to Virnetx's First Amended Complaint** (NO. 607CV80, LED)
- 10 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827533 (Trial Pleading) (E.D.Tex. May 24, 2007) **Plaintiff Virnetx's Reply to Defendant Microsoft's Counterclaims** (NO. 607CV80, LED)
- 11 VIRNETX INC., Plaintiff, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, Involuntary plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 2775842 (Trial Pleading) (E.D.Tex. Jun. 10, 2008) **Plaintiff Virnetx Inc.'s and Science Applications International Corporation's First Amended Complaint for Patent Infringement** (NO. 607CV00080)

E.D.Tex. Expert Testimony

- 12 VIRNETX, INC., v. MICROSOFT CORPORATION., 2008 WL 7465386 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) (**Report or Affidavit of Mark T. Jones, Ph.D.**) (NO. 07CV00080)
- 13 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465387 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **Exhibit E: Summary of Opinions of Dr. David B. Johnson Regarding Claim Construction** (NO. 607-CV-80, LED)
- 14 VIRNETX, INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465388 (Partial Expert Testimony) (E.D.Tex. Dec. 17, 2008) **Oral & Videotaped Deposition of David P. Johnson, Ph.D.** (NO. 607CV80, LED)
- 15 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5631263 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 16 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465389 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 17 VIRNETX INC., Plaintiff, Science Applications International Corporation, Involuntary Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5653416 (Expert Report and Affidavit) (E.D.Tex. Dec. 30, 2008) **Declaration of Mark T. Jones, Ph.D.** (NO. 607CV80, LED)
- 18 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 423638 (Expert Report and Affidavit) (E.D.Tex. Jan. 20, 2009) **Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 19 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732176 (Expert Report and Affidavit)

- (E.D.Tex. Feb. 3, 2009) **Reply Declaration of Mark T. Jones, Ph.D** (NO. 607CV80, LED)
- 20 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732177 (Expert Report and Affidavit) (E.D.Tex. Feb. 10, 2009) **Reply Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 21 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732178 (Expert Report and Affidavit) (E.D.Tex. Dec. 18, 2009) **Declaration of Dr. Stephen Wicker in Support of Microsoft's Motion for Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607-CV-80, LED)

E.D.Tex. Trial Motions, Memoranda And Affidavits

- 22 VIRNETX INC., Plaintiff , SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, Involuntary plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5531230 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Dec. 30, 2008) **Plaintiff Virnetx Inc.'s Opening Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV00080)
- 23 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155346 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Jan. 20, 2009) **Microsoft's Responsive Claim Construction Brief** (NO. 607-CV-80, LED)
- 24 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155347 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 3, 2009) **Plaintiff Virnetx Inc.'s Reply Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV80, LED)
- 25 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155348 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 10, 2009) **Microsoft's Sur-Reply Claim Construction Brief** (NO. 607-CV-80, LED)
- 26 VIRNETX INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 4654324 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Sep. 3, 2009) **Plaintiff Virnetx Inc.'s Response to Defendant Microsoft Corporation's Motion for Clarification to Amend Appendix B to Claim Construction Opinion** (NO. 607CV80(LED))
- 27 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5819696 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Dec. 18, 2009) **Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607CV00080)

E.D.Tex.

- 28 Mark T. Jones, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914105 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of Mark T. Jones** (NO. 07CV00080)
- 29 David B. Johnson, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007

WL 6914106 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of David B. Johnson** (NO. 07CV00080)

E.D.Tex. Trial Filings

- 30 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827534 (Trial Filing) (E.D.Tex. Aug. 29, 2007) **Joint Conference Report** (NO. 607CV80, LED)
- 31 VIRNETX INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5356442 (Trial Filing) (E.D.Tex. Oct. 31, 2008) **Joint Claim Construction and Prehearing Statement** (NO. 607CV80, LED)

E.D.Tex. Verdicts, Agreements and Settlements

- 32 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2010 WL 1046839 (Verdict, Agreement and Settlement) (E.D.Tex. Jan. 14, 2010) **Stipulation of Dismissal** (NO. 607-CV-80, LED)
- 33 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2010 WL 1046840 (Verdict, Agreement and Settlement) (E.D.Tex. Jan. 14, 2010) **Joint Stipulation Regarding Microsoft's Inequitable Conduct Counterclaims and Affirmative Defenses** (NO. 607-CV-80, LED)

Dockets (U.S.A.)

E.D.Tex.

- 34 VIRNETX, INC. v. MICROSOFT CORPORATION, NO. 6:07cv00080 (Docket) (E.D.Tex. Feb. 15, 2007)

Expert Court Documents (U.S.A.)

E.D.Tex.

- 35 VirnetX Inc. v. Microsoft Corp., 2010 WL 1213036 (Verdict and Settlement Summary) (E.D.Tex. Mar. 16, 2010) (NO. 607-CV-80)

E.D.Tex. Expert Testimony

- 36 VIRNETX, INC., v. MICROSOFT CORPORATION., 2008 WL 7465386 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) (**Report or Affidavit of Mark T. Jones, Ph.D.**) (NO. 07CV00080)
- 37 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465387 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **Exhibit E: Summary of Opinions of Dr. David B. Johnson Regarding Claim Construction** (NO. 607-CV-80, LED)
- 38 VIRNETX, INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465388 (Partial Expert Testimony) (E.D.Tex. Dec. 17, 2008) **Oral & Videotaped Deposition of David**

- P. Johnson, Ph.D.** (NO. 607CV80, LED)
- 39 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5631263 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 40 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465389 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 41 VIRNETX INC., Plaintiff, Science Applications International Corporation, Involuntary Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5653416 (Expert Report and Affidavit) (E.D.Tex. Dec. 30, 2008) **Declaration of Mark T. Jones, Ph.D.** (NO. 607CV80, LED)
- 42 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 423638 (Expert Report and Affidavit) (E.D.Tex. Jan. 20, 2009) **Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 43 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732176 (Expert Report and Affidavit) (E.D.Tex. Feb. 3, 2009) **Reply Declaration of Mark T. Jones, Ph.D** (NO. 607CV80, LED)
- 44 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732177 (Expert Report and Affidavit) (E.D.Tex. Feb. 10, 2009) **Reply Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 45 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732178 (Expert Report and Affidavit) (E.D.Tex. Dec. 18, 2009) **Declaration of Dr. Stephen Wicker in Support of Microsoft's Motion for Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607-CV-80, LED)

E.D.Tex.

- 46 Mark T. Jones, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914105 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of Mark T. Jones** (NO. 07CV00080)
- 47 David B. Johnson, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914106 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of David B. Johnson** (NO. 07CV00080)

Patent Family

- 48 INFORMATION TRANSMISSION INVOLVES COMPARING DISCRIMINATOR VALUE FOR EACH RECEIVED DATA PACKET WITH SET OF VALID DISCRIMINATOR VALUES, ACCEPTING RECEIVED DATA PACKET FOR FURTHER PROCESSING WHILE DETECTING MATCH, Derwent World Patents Legal 2000-399393

Assignments

- 49 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DE-

TAILS). Number of Pages: 005, (DATE RECORDED: Jan 10, 2007)
50 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DE-
TAILS). Number of Pages: 003, (DATE RECORDED: Nov 07, 2003)

Patent Status Files

- .. Request for Re-Examination, (OG DATE: Mar 02, 2010)
- .. Certificate of Correction, (OG DATE: Aug 28, 2007)

Docket Summaries

- 53 VIRNETX INC. v. CISCO SYSTEMS, INC. ET AL, (E.D.TEX. Aug 11, 2010) (NO. 6:10CV00417), (35 USC 271 PATENT INFRINGEMENT)
- 54 VIRNETX INC. v. MICROSOFT CORPORATION, (E.D.TEX. Mar 17, 2010) (NO. 6:10CV00094), (35 USC 271 PATENT INFRINGEMENT)

Litigation Alert

- 55 Derwent LitAlert P2010-35-19 (Aug 11, 2010) Action Taken: complaint for PATENT IN-
FRINGEMENT
- 56 Derwent LitAlert P2010-13-31 (Mar 17, 2010) Action Taken: complaint

Prior Art (Coverage Begins 1976)

- C** 57 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 7010604 Assignee: Science Applications International, (U.S. PTO Utility 2006)
- H** 58 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6502135 Assignee: Science Applications International, (U.S. PTO Utility 2002)
- C** 59 APPARATUS AND METHOD FOR ESTABLISHING A CRYPTOGRAPHIC LINK BETWEEN ELEMENTS OF A SYSTEM, US PAT 5787172 Assignee: The Merdan Group, Inc., (U.S. PTO Utility 1998)
- C** 60 AUTOCONFIGURABLE METHOD AND SYSTEM HAVING AUTOMATED DOWNLOADING, US PAT 5870610 Assignee: Siemens Business Communication Systems,, (U.S. PTO Utility 1999)
- C** 61 CRYPTOGRAPHIC KEY MANAGEMENT APPARATUS AND METHOD, US PAT 5341426 Assignee: Motorola, Inc., (U.S. PTO Utility 1994)
- C** 62 DOMAIN NAME ROUTING, US PAT 6119171 Assignee: IP Dynamics, Inc., (U.S. PTO Utility 2000)
- C** 63 DOMAIN NAME SYSTEM LOOKUP ALLOWING INTELLIGENT CORRECTION OF SEARCHES AND PRESENTATION OF AUXILIARY INFORMATION, US PAT 6332158 (U.S. PTO Utility 2001)
- C** 64 DYNAMIC NETWORK ADDRESS UPDATING, US PAT 6243749 Assignee: Cisco Techno-

- logy, Inc., (U.S. PTO Utility 2001)
- C 65 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 6052788 Assignee: Network Engineering Software, Inc., (U.S. PTO Utility 2000)
 - C 66 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 5898830 Assignee: Network Engineering Software, (U.S. PTO Utility 1999)
 - C 67 MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS, US PAT 5905859 Assignee: International Business Machines, (U.S. PTO Utility 1999)
 - C 68 METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION, US PAT 5796942 Assignee: Computer Associates International, Inc., (U.S. PTO Utility 1998)
 - C 69 METHOD AND APPARATUS FOR CLIENT-HOST COMMUNICATION OVER A COMPUTER NETWORK, US PAT 6119234 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 2000)
 - C 70 METHOD AND APPARATUS FOR CONFIGURING A VIRTUAL PRIVATE NETWORK, US PAT 6226751 Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2001)
 - C 71 METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM, US PAT 5892903 Assignee: Internet Security Systems, Inc., (U.S. PTO Utility 1999)
 - C 72 METHOD AND APPARATUS FOR AN INTERNET PROTOCOL (IP) NETWORK CLUSTERING SYSTEM, US PAT 6006259 Assignee: Network Alchemy, Inc., (U.S. PTO Utility 1999)
 - C 73 METHOD AND APPARATUS FOR A KEY-MANAGEMENT SCHEME FOR INTERNET PROTOCOLS, US PAT 5588060 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1996)
 - C 74 METHOD AND APPARATUS FOR MANAGING A VIRTUAL PRIVATE NETWORK, US PAT 6079020 Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2000)
 - C 75 METHOD AND APPARATUS FOR PROVIDING NETWORK ACCESS CONTROL USING A DOMAIN NAME SYSTEM, US PAT 6256671 Assignee: Nortel Networks Limited, (U.S. PTO Utility 2001)
 - C 76 METHOD AND APPARATUS FOR PROVIDING A VIRTUAL PRIVATE NETWORK, US PAT 6092200 Assignee: Novell, Inc., (U.S. PTO Utility 2000)
 - C 77 METHOD AND PROTOCOL FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION, US PAT 6353614 Assignee: 3Com Corporation, (U.S. PTO Utility 2002)
 - C 78 METHOD AND SYSTEM FOR AUTOMATIC DISCOVERY OF NETWORK SERVICES, US PAT 6286047 Assignee: Hewlett-Packard Company, (U.S. PTO Utility 2001)
 - C 79 MULTI-ACCESS VIRTUAL PRIVATE NETWORK, US PAT 6158011 Assignee: V-One Corporation, (U.S. PTO Utility 2000)
 - C 80 NETWORK COMMUNICATIONS ADAPTER WITH DUAL INTERLEAVED MEMORY BANKS SERVICING MULTIPLE PROCESSORS, US PAT 4933846 Assignee: Network Systems Corporation, (U.S. PTO Utility 1990)
 - C 81 NETWORK WITH SECURE COMMUNICATIONS SESSIONS, US PAT 5689566 (U.S. PTO Utility 1997)

- H** 82 POLICY CACHING METHOD AND APPARATUS FOR USE IN A COMMUNICATION DEVICE BASED ON CONTENTS OF ONE DATA UNIT IN A SUBSET OF RELATED DATA UNITS, US PAT 5842040 Assignee: Storage Technology Corporation, (U.S. PTO Utility 1998)
- C** 83 SECURE DELIVERY OF INFORMATION IN A NETWORK, US PAT 6178505 Assignee: Internet Dynamics, Inc., (U.S. PTO Utility 2001)
- C** 84 SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY, US PAT 5805801 Assignee: International Business Machines, (U.S. PTO Utility 1998)
- C** 85 SYSTEM AND METHOD FOR MANAGING SECURITY OBJECTS, US PAT 6330562 Assignee: International Business Machines, (U.S. PTO Utility 2001)
- C** 86 SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE, US PAT 5878231 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1999)
- C** 87 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR MULTIPLE-ENTRY POINT VIRTUAL POINT OF SALE ARCHITECTURE, US PAT 6178409 Assignee: VeriFone, Inc., (U.S. PTO Utility 2001)
- C** 88 VIRTUAL PRIVATE NETWORK SYSTEM OVER PUBLIC MOBILE DATA NETWORK AND VIRTUAL LAN, US PAT 6016318 Assignee: NEC Corporation, (U.S. PTO Utility 2000)

Single Search - with Terms and Connectors

Enter keywords - Search multiple dockets & documents [View Demo](#)
[Search Tips](#)

My CourtLink | Search | Dockets & Documents | Track | Alert | Strategic Profiles | My Account

[Search](#) > [Patent Search](#) > **Litigation involving patent 7188180**

Click a docket number below to view a docket.

Patent Search Results

[Edit Search](#)

Results: 2 cases and their patents, totaling 2 items.

This search was run on 12/1/2010

[Printer Friendly List](#)
[Email List](#)
[Customize List](#)

Items 1 to 2 of 2

<input type="checkbox"/>	Patent	Class	Subclass	Description	Court	Docket Number	Filed	Date Retrieved
<input type="checkbox"/>	7,188,180	709	227	Virnetx Inc v. Cisco Systems, Inc et al	US-DIS-TXED	6:10cv417	8/11/2010	11/2/2010
<input type="checkbox"/>	7,188,180	709	227	Virnetx Inc v. Microsoft Corporation	US-DIS-TXED	6:10cv94	3/17/2010	7/15/2010

Items 1 to 2 of 2

[Printer Friendly List](#)
[Email List](#)
[Customize List](#)



US District Court Civil Docket

U.S. District - Texas Eastern
(Tyler)

6:10cv417

Virnetx Inc v. Cisco Systems, Inc et al

This case was retrieved from the court on Tuesday, November 02, 2010

Date Filed: 08/11/2010	Class Code:
Assigned To: Judge Leonard Davis	Closed: No
Referred To:	Statute: 35:271
Nature of suit: Patent (830)	Jury Demand: Both
Cause: Patent Infringement	Demand Amount: \$0
Lead Docket: None	NOS Description: Patent
Other Docket: None	
Jurisdiction: Federal Question	

Litigants

Virnetx Inc
Plaintiff

Attorneys

Douglas A Cawley
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Ameet A Modi
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ i>

Cisco Systems, Inc
Defendant

Email: AMODI@DESMARAISLLP.COM

Dmitriy Kheyfits
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: DKHEYFITS@DESMARAISLLP.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

John M Desmarais
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: JDESMARAIS@DESMARAISLLP.COM

Michael P Stadnick
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: MSTADNICK@DESMARAISLLP.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Tamir Packin
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: TPACKIN@DESMARAISLLP.COM

Danny Lloyd Williams
[COR LD NTC]
Williams Morgan & Amerson
10333 Richmond
Suite 1100

Apple Inc
Defendant

Houston , TX 77042
USA
713/ 934-4060
Fax: 17139347011
Email: Dwilliams@wmalaw.com

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

Kyung Kim
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4080
Fax: 713/ 934-7011
Email: DKIM@WMALAW.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Ruben Singh Bains
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4064
Fax: 713/ 934-7011
Email: Rbains@wmalaw.com

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC

Aastra Technologies Ltd
Defendant

901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Nec Corporation
Defendant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Nec Corporation of America
Defendant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622

Aastra USA, Inc
Defendant

Email: RKATZ@PATTONROBERTS.COM

Nec Corporation of America
Counter Claimant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Nec Corporation
Counter Claimant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005

USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1705
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Douglas A Cawley
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]

Virnetx Inc
Counter Defendant

Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Counter Claimant

Ameet A Modi
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: AMODI@DESMARAISLLP.COM

Dmitriy Kheyfits
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: DKHEYFITS@DESMARAISLLP.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

John M Desmarais
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: JDESMARAIS@DESMARAISLLP.COM

Michael P Stadnick
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: MSTADNICK@DESMARAISLLP.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Tamir Packin
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401

<i>pro Hac Vice</ I>
Email: TPACKIN@DESMARAISLLP.COM

Virnetx Inc
Counter Defendant

Douglas A Cawley
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court

Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckkoolsmith.com

Danny Lloyd Williams
[COR LD NTC]
Williams Morgan & Amerson
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4060
Fax: 17139347011
Email: Dwilliams@wmalaw.com

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

Kyung Kim
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4080
Fax: 713/ 934-7011
Email: DKIM@WMALAW.COM

Roger Brian Craft
[COR LD NTC]

Apple Inc
Counter Claimant

Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Ruben Singh Bains
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4064
Fax: 713/ 934-7011
Email: Rbains@wmalaw.com

Douglas A Cawley
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044

Virnetx Inc
Counter Defendant

Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826

Aastra Technologies Ltd
Counter Claimant

Email: JHYLAND@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Virnetx Inc
Counter Defendant

Douglas A Cawley
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassidy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500

Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300

Aastra USA, Inc
Counter Claimant

Virnetx Inc
Counter Defendant

Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Douglas A Cawley
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy

[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckkoolsmith.com

Date	#	Proceeding Text
08/11/2010	1	COMPLAINT against Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America (Filing fee \$ 350 receipt number 0540-2618483.), filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Exhibit E, # 6 Civil Cover Sheet)(Cawley, Douglas) (Entered: 08/11/2010)
08/11/2010	--	Judge Leonard Davis added. (mll,) (Entered: 08/12/2010)
08/12/2010	2	CORPORATE DISCLOSURE STATEMENT filed by VirnetX Inc. identifying Corporate Parent VirnetX Holding Corporation for VirnetX Inc.. (Cawley, Douglas) (Entered: 08/12/2010)
08/12/2010	3	E-GOV SEALED SUMMONS Issued as to Apple Inc. (kls,) (Entered: 08/12/2010)
08/12/2010	4	E-GOV SEALED SUMMONS Issued as to Aastra Technologies Ltd. (kls,) (Entered: 08/12/2010)
08/12/2010	5	E-GOV SEALED SUMMONS Issued as to Cisco Systems, Inc. (kls,) (Entered: 08/12/2010)
08/12/2010	6	Notice of Filing of Patent/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. Patent and Trademark Office. (Cawley, Douglas) (Entered: 08/12/2010)
08/12/2010	7	E-GOV SEALED SUMMONS Issued as to NEC Corporation. (kls,) (Entered: 08/12/2010)
08/12/2010	8	E-GOV SEALED SUMMONS Issued as to Aastra USA, Inc. (kls,) (Entered: 08/12/2010)
08/12/2010	9	E-GOV SEALED SUMMONS Issued as to NEC Corporation of America. (kls,) (Entered: 08/12/2010)
08/17/2010	10	NOTICE of Attorney Appearance by Samuel Franklin Baxter on behalf of VirnetX Inc. (Baxter, Samuel) (Entered: 08/17/2010)
08/17/2010	11	NOTICE of Attorney Appearance by Luke Fleming McLeroy on behalf of VirnetX Inc. (McLeroy, Luke) (Entered: 08/17/2010)
08/17/2010	12	NOTICE of Attorney Appearance by Bradley Wayne Caldwell on behalf of VirnetX Inc. (Caldwell, Bradley) (Entered: 08/17/2010)
08/17/2010	13	NOTICE of Attorney Appearance by Jason Dodd Cassidy on behalf of VirnetX Inc. (Cassady, Jason) (Entered: 08/17/2010)

09/01/2010 14 Unopposed MOTION for Extension of Time to File Answer re 1 Complaint, or Otherwise Respond by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order)(Craft, Roger) (Entered: 09/01/2010)

09/01/2010 15 Unopposed MOTION for Extension of Time to File Answer re 1 Complaint, by Apple Inc.. (Attachments: # 1 Text of Proposed Order)(Craft, Roger) (Entered: 09/01/2010)

09/01/2010 16 NOTICE of Attorney Appearance by Eric Hugh Findlay on behalf of Cisco Systems, Inc. (Findlay, Eric) (Entered: 09/01/2010)

09/01/2010 17 NOTICE of Attorney Appearance by Eric Hugh Findlay on behalf of Apple Inc. (Findlay, Eric) (Entered: 09/01/2010)

09/02/2010 18 ORDER granting 14 Motion for Extension of Time to Answer. Deft Cisco Systems Inc shall have to 10-29-2010 to move, answer, or otherwise respond to pltf's Complaint. Signed by Judge Leonard Davis on 09/02/10. cc:attys 9-02-10 (mll,) (Entered: 09/02/2010)

09/02/2010 19 ORDER granting 15 Motion for Extension of Time to Answer. Deft Apple Inc shall have to 10-29-2010 to move, answer, or otherwise respond to pltf's Complaint. Signed by Judge Leonard Davis on 09/02/10. cc:attys 9-02-10 (mll,) (Entered: 09/02/2010)

09/03/2010 20 NOTICE of Attorney Appearance by Phillip Nollin Cockrell on behalf of Aastra Technologies Ltd., Aastra USA, Inc. (Cockrell, Phillip) (Entered: 09/03/2010)

09/03/2010 21 NOTICE of Attorney Appearance by Robert David Katz on behalf of Aastra Technologies Ltd., Aastra USA, Inc. (Katz, Robert) (Entered: 09/03/2010)

09/03/2010 22 NOTICE of Attorney Appearance by Jon Bentley Hyland on behalf of Aastra Technologies Ltd., Aastra USA, Inc. (Hyland, Jon) (Entered: 09/03/2010)

09/03/2010 23 DOCUMENT FILED IN ERROR. PLEASE DISREGARD.*** Defendant's Unopposed First Application for Extension of Time to Answer, Move or Otherwise Respond to Complaint re Aastra Technologies Ltd., Aastra USA, Inc.. (Hyland, Jon) Modified on 9/7/2010 (mjc,). (Entered: 09/03/2010)

09/03/2010 27 APPLICATION to Appear Pro Hac Vice by Attorney Robert M Masters for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/07/2010)

09/03/2010 28 APPLICATION to Appear Pro Hac Vice by Attorney Bhaskar Kakarla for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/07/2010)

09/03/2010 29 APPLICATION to Appear Pro Hac Vice by Attorney Brock S Weber for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/07/2010)

09/07/2010 -- ***FILED IN ERROR. Document # 23 , Defendant's First Unopposed Application for Extension of Time. DOCUMENT FILED USING INCORRECT DOCKET EVENT. PLEASE IGNORE.*** (mjc,) (Entered: 09/07/2010)

09/07/2010 24 Agreed MOTION for Extension of Time to File Answer re 1 Complaint, by Aastra Technologies Ltd., Aastra USA, Inc.. (Attachments: # 1 Text of Proposed Order)(Hyland, Jon) (Entered: 09/07/2010)

09/07/2010 25 E-GOV SEALED SUMMONS Issued as to NEC Corporation of America. (kls,) (Entered: 09/07/2010)

09/07/2010 26 E-GOV SEALED SUMMONS Issued as to NEC Corporation. (kls,) (Entered: 09/07/2010)

09/08/2010 30 ORDER granting 24 Motion for Extension of Time to Answer. Aastra defts will have to 10-29-2010 to answer, move or otherwise respond to pltf's Complaint. Signed by Judge Leonard Davis on 09/08/10. cc:attys 9-08-10 (mll,) (Entered: 09/08/2010)

09/09/2010 31 NOTICE of Attorney Appearance by Robert M Parker on behalf of VirnetX Inc. (Parker, Robert) (Entered: 09/09/2010)

09/09/2010 32 NOTICE of Attorney Appearance by Robert Christopher Bunt on behalf of VirnetX Inc. (Bunt, Robert) (Entered: 09/09/2010)

09/09/2010 33 NOTICE of Attorney Appearance by Charles Ainsworth on behalf of VirnetX Inc. (Ainsworth, Charles) (Entered: 09/09/2010)

09/09/2010 34 NOTICE of Attorney Appearance by Andrew Thompson Gorham on behalf of VirnetX Inc. (Gorham, Andrew) (Entered: 09/09/2010)

09/09/2010 35 NOTICE of Attorney Appearance by Daniel R Pearson on behalf of VirnetX Inc. (Pearson, Daniel) (Entered: 09/09/2010)

09/16/2010 36 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Aastra Technologies Ltd. personally served on 8/20/2010 by Process Server Andrew Kovacs on Jamshid Rezaei, Director IT designated to accept process of service, answer due 9/10/2010. (ehs,) (Entered: 09/16/2010)

09/16/2010 37 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Aastra USA, Inc. personally served on Sue Vertrees designated by law to accept process of service served on 8/18/2010, answer due 9/8/2010. (ehs,) (Entered: 09/16/2010)

09/16/2010 38 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Apple Inc. served on 8/18/2010 by serving Registered Agent Meagan Nichols, answer due 9/8/2010. (ehs,) (Entered: 09/16/2010)

09/16/2010 39 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Cisco Systems, Inc. personally served on 8/18/2010 Bradley Ellison, person authorized to accept service of process, answer due 9/8/2010. (ehs,) (Entered: 09/16/2010)

09/16/2010 40 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. NEC Corporation of America personally served on 8/19/2010 on Dionne Miles, Managing Agent authorized by law to accept service of process, answer due

9/9/2010. (ehs,) (Entered: 09/16/2010)

09/16/2010 41 APPLICATION to Appear Pro Hac Vice by Attorney Timothy P Cremen for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/16/2010)

09/28/2010 42 NEC Corporation's Unopposed First Application for Extension of Time to Answer Complaint (McSwane, Douglas). (Entered: 09/28/2010)

09/28/2010 43 NEC Corporation of America's Unopposed First Application for Extension of Time to Answer Complaint (McSwane, Douglas) (Entered: 09/28/2010)

09/29/2010 -- Defendant's Unopposed First Application for Extension of Time to Answer Complaint 42 is granted pursuant to Local Rule CV-12 for NEC Corporation to 10/29/2010. 10 Days Granted for Deadline Extension.(mll,) (Entered: 09/29/2010)

09/29/2010 -- Defendant's Unopposed First Application for Extension of Time to Answer Complaint 43 is granted pursuant to Local Rule CV-12 for NEC Corporation of America to 10/29/2010. 30 Days Granted for Deadline Extension. (mll,) (Entered: 09/29/2010)

10/06/2010 44 NOTICE of Attorney Appearance by Danny Lloyd Williams on behalf of Apple Inc. (Williams, Danny) (Entered: 10/06/2010)

10/06/2010 45 NOTICE of Attorney Appearance by Ruben Singh Bains on behalf of Apple Inc. (Bains, Ruben) (Entered: 10/06/2010)

10/06/2010 46 NOTICE of Attorney Appearance by Kyung Kim on behalf of Apple Inc. (Kim, Kyung) (Entered: 10/06/2010)

10/26/2010 47 APPLICATION to Appear Pro Hac Vice by Attorney Tamir Packin for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)

10/26/2010 48 APPLICATION to Appear Pro Hac Vice by Attorney Ameet A Modi for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)

10/26/2010 49 APPLICATION to Appear Pro Hac Vice by Attorney Dmitriy Kheyfits for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)

10/26/2010 50 APPLICATION to Appear Pro Hac Vice by Attorney John M Desmarais for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)

10/26/2010 51 APPLICATION to Appear Pro Hac Vice by Attorney Michael P Stadnick for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)

10/29/2010 52 NEC Corp and NEC Corp of America's ANSWER to 1 Complaint, and , COUNTERCLAIM against VirnetX Inc. by NEC Corporation of America, NEC Corporation.(McSwane, Douglas) (Entered: 10/29/2010)

10/29/2010 53 Cisco Systems, Inc.'s ANSWER to 1 Complaint, and , COUNTERCLAIM against VirnetX Inc. by Cisco Systems, Inc..(Findlay, Eric) (Entered: 10/29/2010)

10/29/2010 54 CORPORATE DISCLOSURE STATEMENT filed by Cisco Systems, Inc. identifying Corporate Parent None for Cisco Systems, Inc.. (Findlay, Eric) (Entered: 10/29/2010)

10/29/2010 55 ANSWER to 1 Complaint, AFFIRMATIVE DEFENSES , COUNTERCLAIM against VirnetX Inc. by Apple Inc.. (Williams, Danny) (Entered: 10/29/2010)

10/29/2010 56 CORPORATE DISCLOSURE STATEMENT filed by Apple Inc. (Williams, Danny) (Entered: 10/29/2010)

10/29/2010 57 Aastra Technologies Limited's ANSWER to 1 Complaint, AFFIRMATIVE DEFENSES , COUNTERCLAIM against VirnetX Inc. by Aastra Technologies Ltd..(Cockrell, Phillip) (Entered: 10/29/2010)

10/29/2010 58 CORPORATE DISCLOSURE STATEMENT filed by Aastra Technologies Ltd. (Cockrell, Phillip) (Entered: 10/29/2010)

10/29/2010 59 Aastra USA Inc's ANSWER to 1 Complaint, AFFIRMATIVE DEFENSES , COUNTERCLAIM against VirnetX Inc. by Aastra USA, Inc..(Cockrell, Phillip) (Entered: 10/29/2010)

10/29/2010 60 CORPORATE DISCLOSURE STATEMENT filed by Aastra USA, Inc. (Cockrell, Phillip) (Entered: 10/29/2010)

11/02/2010 61 CORPORATE DISCLOSURE STATEMENT filed by NEC Corporation, NEC Corporation of America (McSwane, Douglas) (Entered: 11/02/2010)

US District Court Civil Docket

U.S. District - Texas Eastern
(Tyler)

6:10cv94

Virnetx Inc v. Microsoft Corporation

This case was retrieved from the court on Thursday, July 15, 2010

Date Filed: 03/17/2010	Class Code: CLOSED
Assigned To: Judge Leonard Davis	Closed: Yes
Referred To:	Statute: 35:271
Nature of suit: Patent (830)	Jury Demand: Plaintiff
Cause: Patent Infringement	Demand Amount: \$0
Lead Docket: None	NOS Description: Patent
Other Docket: None	
Jurisdiction: Federal Question	

Litigants

Virnetx Inc
Plaintiff

Attorneys

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Douglas A Cawley
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Microsoft Corporation
Defendant

Matthew Douglas Powers
[COR LD NTC]
Weil Gotshal & Manges-Redwood Shores
201 Redwood Shores Parkway
5TH Floor
Redwood City , CA 94065
USA
650-802-3200
Fax: 650-802-3100
Email: MATTHEW.POWERS@WEIL.COM

Amber Hatfield Rovner
[COR LD NTC]
Weil Gotshal & Manges-Houston
700 Louisiana
Suite 1600
Houston , TX 77002-2784
USA
201-386-2955
Fax: 713-223-9511
Email: AMBER.ROVNER@WEIL.COM

Daniel James Booth
[COR LD NTC]
Weil Gotshal & Manges-Houston
700 Louisiana
Suite 1600
Houston , TX 77002-2784
USA
713-546-5135
Fax: 713-224-9511
Email: DANIEL.BOOTH@WEIL.COM

Elizabeth S Weiswasser
[COR LD NTC]
Weil Gotshal & Manges-NY
767 Fifth Avenue
New York , NY 10153-0119
USA
212-310-8022
Fax: 212-310-8007
<i>pro Hac Vice</ I>
Email: ELIZABETH.WEISWASSER@WEIL.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

Jared B Bobrow
[COR LD NTC]
Weil Gotshal & Manges-Redwood Shores
201 Redwood Shores Parkway
5TH Floor
Redwood City , CA 94065
USA
605/ 802-3034
Fax: 605/ 802-3100
<i>pro Hac Vice</ I>
Email: JARED.BOBROW@WEIL.COM

Paul T Ehrlich
[COR LD NTC]
Weil Gotshal & Manges-Redwood Shores
201 Redwood Shores Parkway
5TH Floor
Redwood City , CA 94065
USA

650/ 802-3227
Fax: 650/ 802-3100
Email: PAUL.EHRLICH@WEIL.COM

Robert Lewis Gerrity
[COR LD NTC]
Weil Gotshal & Manges-Redwood Shores
201 Redwood Shores Parkway
5TH Floor
Redwood City , CA 94065
USA
650/ 802-3000
Fax: 650/ 802-3100
<i>pro Hac Vice</ I>
Email: ROBERT.GERRITY@WEIL.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Thomas B King
[COR LD NTC]
Weil Gotshal & Manges-Redwood Shores
201 Redwood Shores Parkway
5TH Floor
Redwood City , CA 94065
USA
605/ 802-3000
Fax: 605/ 802-3100
<i>pro Hac Vice</ I>
Email: THOMAS.KING@WEIL.COM

Date	#	Proceeding Text
03/17/2010	1	COMPLAINT against Microsoft Corporation (Filing fee \$ 350 receipt number 0540-2403564.), filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Civil Cover Sheet)(Cawley, Douglas) (Entered: 03/17/2010)
03/17/2010	2	CORPORATE DISCLOSURE STATEMENT filed by VirnetX Inc. identifying Corporate Parent None for VirnetX Inc.. (Cawley, Douglas) (Entered: 03/17/2010)
03/17/2010	--	Judge Leonard Davis added. (mll,) (Entered: 03/18/2010)
03/22/2010	3	E-GOV SEALED SUMMONS Issued as to Microsoft Corporation, and emailed to pltf for service. (mll,) (Entered: 03/22/2010)
03/24/2010	4	Unopposed MOTION for Extension of Time to File Answer re 1 Complaint Agreed Motion for Extension of Time to Answer, Move, or Otherwise Respond to Plaintiff's Complaint by Microsoft Corporation. (Attachments: # 1 Text of Proposed Order)(Findlay, Eric) (Entered: 03/24/2010)
03/25/2010	5	ORDER granting 4 Motion for Extension of Time to Answer. Microsoft shall answer, move, or otherwise respond to pltf's Complaint by 5-10-2010. Signed by Judge Leonard Davis on 03/25/10. cc:attys 3-25-10 (mll,) (Entered: 03/25/2010)
03/26/2010	6	CORPORATE DISCLOSURE STATEMENT filed by Microsoft Corporation identifying Corporate Parent None for Microsoft Corporation. (Findlay, Eric) (Entered: 03/26/2010)
03/30/2010	7	NOTICE of Attorney Appearance by Luke Fleming McLeroy on behalf of VirnetX Inc. (McLeroy, Luke) (Entered: 03/30/2010)
03/30/2010	8	NOTICE of Attorney Appearance by Jason Dodd Cassady on behalf of VirnetX Inc. (Cassady, Jason) (Entered: 03/30/2010)
03/30/2010	9	NOTICE of Attorney Appearance by Bradley Wayne Caldwell on behalf of VirnetX Inc. (Caldwell, Bradley) (Entered: 03/30/2010)
04/21/2010	10	NOTICE of Attorney Appearance by Roger Brian Craft on behalf of Microsoft Corporation (Craft, Roger) (Entered: 04/21/2010)
04/26/2010	11	ORDER that plaintiff file a notice that the case is ready for scheduling conference when all of the defendants have either answered or filed a motion to transfer or dismiss. The notice shall be filed within five days of the last remaining defendant's answer or motion. Signed by Judge Leonard Davis on 04/26/10. cc:attys 4-27-10

(mll,) (Entered: 04/27/2010)

05/05/2010 12 NOTICE of Attorney Appearance by Matthew Douglas Powers on behalf of Microsoft Corporation (Powers, Matthew) (Entered: 05/05/2010)

05/05/2010 13 NOTICE of Attorney Appearance by Daniel James Booth on behalf of Microsoft Corporation (Booth, Daniel) (Entered: 05/05/2010)

05/05/2010 14 NOTICE of Attorney Appearance by Paul T Ehrlich on behalf of Microsoft Corporation (Ehrlich, Paul) (Entered: 05/05/2010)

05/05/2010 15 NOTICE of Attorney Appearance by Amber Hatfield Rovner on behalf of Microsoft Corporation (Rovner, Amber) (Entered: 05/05/2010)

05/06/2010 16 APPLICATION to Appear Pro Hac Vice by Attorney Jared B Bobrow for Microsoft Corporation. (mll,) (Entered: 05/06/2010)

05/06/2010 17 APPLICATION to Appear Pro Hac Vice by Attorney Robert Lewis Gerrity for Microsoft Corporation. (mll,) (Entered: 05/06/2010)

05/06/2010 18 APPLICATION to Appear Pro Hac Vice by Attorney Thomas B King for Microsoft Corporation. (mll,) (Entered: 05/06/2010)

05/06/2010 19 APPLICATION to Appear Pro Hac Vice by Attorney Elizabeth S Weiswasser for Microsoft Corporation. (mll,) (Entered: 05/06/2010)

05/07/2010 20 Unopposed MOTION for Extension of Time to File Answer re 1 Complaint Second Agreed Motion for Extention of Time to Answer, Move, or Otherwise Respond to Plaintiff's Complaint by Microsoft Corporation. (Attachments: # 1 Text of Proposed Order)(Booth, Daniel) (Entered: 05/07/2010)

05/07/2010 21 ORDER granting 20 Motion for Extension of Time to Answer. Microsoft shall answer, move, or otherwise respond to pltf's Complaint by 5-24-2010. Signed by Judge Leonard Davis on 05/07/10. cc:attys 5-07-10 (mll,) (Entered: 05/07/2010)

05/18/2010 22 STIPULATION of Dismissal by Microsoft Corporation, VirnetX Inc.. (Attachments: # 1 Text of Proposed Order) (Powers, Matthew) (Entered: 05/18/2010)

05/25/2010 23 ORDER granting 22 Stipulation of Dismissal filed by VirnetX Inc., Microsoft Corporation. All of the claims asserted against Microsoft in this action are dismissed with prejudice. Each party shall bear its own costs, expenses and fees. This is a Final Judgment. Signed by Judge Leonard Davis on 05/24/10. cc:attys 5-25-10 (mll,) (Entered: 05/25/2010)

Copyright © 2010 LexisNexis CourtLink, Inc. All rights reserved.
*** THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY ***



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.
Row 1: 12/472,165, 05/26/2009, Roop C. Jain, R0575-700160, 7171
Row 2: 56885, 7590, 12/01/2010, Siemens Corporation, U0105, Intellectual Property Department, 170 Wood Avenue South, Iselin, NJ 08830
Row 3: EXAMINER: CONLEY, SEAN EVERETT
Row 4: ART UNIT: 1773, PAPER NUMBER
Row 5: MAIL DATE: 12/01/2010, DELIVERY MODE: 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

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	12/03/2010	EXAMINER	
McDermott Will & Emery 600 13th Street, NW Washington, DC 20005-3096			NALVEN, ANDREW L	
			ART UNIT	PAPER NUMBER
			3992	
			MAIL DATE	DELIVERY MODE
			12/03/2010	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

DEC 03 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)

**Right of Appeal Notice
(37 CFR 1.953)**

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 _____

Third Party(ies) on _____

Patent owner and/or third party requester(s) may file a notice of appeal with respect to any adverse decision with payment of the fee set forth in 37 CFR 41.20(b)(1) within **one-month or thirty-days (whichever is longer)**. See MPEP 2671. In addition, a party may file a notice of **cross** appeal and pay the 37 CFR 41.20(b)(1) fee **within fourteen days of service** of an opposing party's timely filed notice of appeal. See MPEP 2672.

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.

If no party timely files a notice of appeal, prosecution on the merits of this reexamination proceeding will be concluded, and the Director of the USPTO will proceed to issue and publish a certificate under 37 CFR 1.997 in accordance with this Office action.

The proposed amendment filed _____ will be entered will not be entered*

*Reasons for non-entry are given in the body of this notice.

- 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 cancelled.
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) or (f). The certified copy has:
 been received. not been received. been filed in Application/Control No. _____.
10. Other _____

Attachments

1. Notice of References Cited by Examiner, PTO-892
2. Information Disclosure Citation, PTO/SB/08
3. _____

RIGHT OF APPEAL NOTICE

The following action addresses claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of US Patent No. 7,188,180 ("the '180 patent").

An Action Closing Prosecution was issued on June 16, 2010.

No response to the Action Closing Prosecution was received.

Status of Claims

Original Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are confirmed.

Rejections Proposed by Requestor – Previously Adopted, Now Not Adopted

1. 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.
2. 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 '180 patent. Specifically, Patent Owner argued that the request and the 1/19/2010 office action did not show that Aventail was published 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.

Art Unit: 3992

3. 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.

4. 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*).

5. 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

Art Unit: 3992

non-conventional domain name system. For this additional reason the proposed rejection is not adopted.

6. 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.

7. 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

8. 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.

9. 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.

10. 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

Art Unit: 3992

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*).

11. 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.

12. 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. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

13. 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

Art Unit: 3992

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*).

14. 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 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

Art Unit: 3992

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.

15. 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.

16. 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

17. 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.

18. 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.

19. 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

Art Unit: 3992

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*).

20. 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.

21. 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.

Art Unit: 3992

22. 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*).

23. 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 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

24. The non-final action mailed on January 19, 2010 is hereby incorporated by reference.

25. 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.

26. 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.

27. 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.

28. 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 was not adopted for the reasons set forth on Pages 22-23 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 Gauntlet. This proposed rejection was not adopted for the reasons set forth on Page 24 of the January 19, 2010 non-final office action.

Art Unit: 3992

30. 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 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*) 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.

Art Unit: 3992

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.

This is a RIGHT OF APPEAL NOTICE (RAN); see MPEP § 2673.02 and § 2674. The decision in this Office action as to the patentability or unpatentability of any original patent claim, any proposed amended claim and any new claim in this proceeding is a FINAL DECISION.

No amendment can be made in response to the Right of Appeal Notice in an *inter partes* reexamination. 37 CFR 1.953(c). Further, no affidavit or other evidence can be submitted in an *inter partes* reexamination proceeding after the right of appeal notice, except as provided in 37 CFR 1.981 or as permitted by 37 CFR 41.77(b)(1). 37 CFR 1.116(f).

Each party has a **thirty-day or one-month time period, whichever is longer**, to file a notice of appeal. The patent owner may appeal to the Board of Patent Appeals and Interferences with respect to any decision adverse to the patentability of any original or proposed amended or new claim of the patent by filing a notice of appeal and paying the fee set forth in 37 CFR 41.20(b)(1). The third party requester may appeal to the Board of Patent Appeals and Interferences with respect to any decision favorable to the patentability of any original or proposed amended or new claim of the patent by filing a notice of appeal and paying the fee set forth in 37 CFR 41.20(b)(1).

In addition, a patent owner who has not filed a notice of appeal may file a notice of cross appeal within **fourteen days of service** of a third party requester's timely filed notice of appeal and pay the fee set forth in 37 CFR 41.20(b)(1). A third party requester who has not filed a

Art Unit: 3992

notice of appeal may file a **notice of cross appeal within fourteen days of service** of a patent owner's timely filed notice of appeal and pay the fee set forth in 37 CFR 41.20(b)(1).

Any appeal in this proceeding must identify the claim(s) appealed, and must be signed by the patent owner (for a patent owner appeal) or the third party requester (for a third party requester appeal), or their duly authorized attorney or agent.

Any party that does not file a timely notice of appeal or a timely notice of cross appeal will lose the right to appeal from any decision adverse to that party, but will not lose the right to file a respondent brief and fee where it is appropriate for that party to do so. If no party files a timely appeal, the reexamination prosecution will be terminated, and the Director will proceed to issue and publish a certificate under 37 CFR 1.997 in accordance with this 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

Art Unit: 3992

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: HNT

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)				ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270	
				APPLICANT Victor Larson		
				FILING DATE December 8, 2009	GROUP 3992	
U.S. PATENT DOCUMENTS						
EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ² of # ¹ row(s)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A100	US	4,933,846	6/12/1990	Humphrey et al.	
	A101	US	4,988,990	1/29/1991	Warrior	
	A102	US	5,276,735	1/4/1994	Boebert et al	
	A103	US	5,329,521	7/12/1994	Walsh et al.	
	A104	US	5,341,426	8/23/1994	Barney et al.	
	A105	US	5,367,643	11/22/1994	Chang et al	
	A106	US	5,559,883	9/24/1996	Williams	
	A107	US	5,561,669	10/1/1996	Lenney et al	
	A108	US	5,588,060	12/24/1996	Aziz	
	A109	US	5,625,626	4/29/1997	Umekita	
	A110	US	5,654,695	8/5/1997	Olnowich et al	
	A111	US	5,682,480	10/28/1997	Nakagawa	
	A112	US	5,689,566	11/18/1997	Nguyen	
	A113	US	5,740,375	4/14/1998	Dunne et al.	
	A114	US	5,774,660	6/30/1998	Brendel et al	
	A115	US	5,787,172	7/28/1998	Arnold	
	A116	US	5,796,942	8/18/1998	Esbensen	
	A117	US	5,805,801	9/8/1998	Holloway et al.	
	A118	US	5,842,040	11/24/1998	Hughes et al.	
	A119	US	5,845,091	12/1/1998	Dunne et al.	
	A120	US	5,867,650	2/2/1998	Osterman	
	A121	US	5,870,610	2/9/1999	Beyda et al.	
	A122	US	5,878,231	5/2/1999	Baehr et al	
	A123	US	5,892,903	4/6/1999	Klaus	
	A124	US	5,905,859	5/18/1999	Holloway et al.	
	A125	US	5,918,019	6/29/1999	Valencia	
	A126	US	5,996,016	11/30/1999	Thalheimer et al.	
	A127	US	6,006,259	12/21/1999	Adelman et al.	
	A128	US	6,006,272	12/21/1999	Aravamudan et al	
	A129	US	6,016,318	1/18/2000	Tomoike	
	A130	US	6,016,512	1/18/2000	Huitema	
	A131	US	6,041,342	3/21/2000	Yamaguchi	
	A132	US	6,061,736	5/9/2000	Rochberger et al	
EXAMINER /Andrew Naalven/				DATE CONSIDERED 11/30/2010		

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)				ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270	
				APPLICANT Victor Larson		
				FILING DATE December 8, 2009	GROUP 3992	
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
	A133	US	6,092,200	7/18/2000	Muniyappa et al.	
	A134	US	6,119,234	9/12/2000	Aziz et al.	
	A135	US	6,147,976	11/14/2000	Shand et al.	
	A136	US	6,157,957	12/5/2000	Berthaud	
	A137	US	6,158,011	12/5/2000	Chen et al.	
	A138	US	6,168,409	1/2/2001	Fare	
	A139	US	6,175,867	1/16/2001	Taghadoss	
	A140	US	6,178,409	1/23/2001	Weber et al.	
	A141	US	6,178,505	1/23/2001	Schneider et al	
	A142	US	6,179,102	1/30/2001	Weber, et al.	
	A143	US	6,222,842	4/24/2001	Sasyan et al.	
	A144	US	6,233,618	5/15/2001	Shannon	
	A145	US	6,243,360	6/5/2001	Basilico	
	A146	US	6,243,749	6/5/2001	Sitaraman et al.	
	A147	US	6,243,754	6/5/2001	Guerin et al	
	A148	US	6,256,671	7/3/2001	Strentzsch et al.	
	A149	US	6,263,445	7/17/2001	Blumenau	
	A150	US	6,286,047	9/4/2001	Ramanathan et al	
	A151	US	6,301,223	10/9/2001	Hrastar et al	
	A152	US	6,308,274	10/23/2001	Swift	
	A153	US	6,311,207	10/30/2001	Mighdoll et al	
	A154	US	6,324,161	11/27/2001	Kirch	
	A155	US	6,330,562	12/11/2001	Boden et al.	
	A156	US	6,332,158	12/18/2001	Risley et al.	
	A157	US	6,353,614	3/5/2002	Borella et al.	
	A158	US	6,430,155	8/6/2002	Davie et al	
	A159	US	6,430,610	8/6/2002	Carter	
	A160	US	6,487,598	11/26/2002	Valencia	
	A161	US	6,505,232	1/7/2003	Mighdoll et al	
	A162	US	6,510,154	1/21/2003	Mayer et al	
	A163	US	6,549,516	4/15/2003	Albert et al	
	A164	US	6,571,296	5/27/2002	Dillon	
	A165	US	6,571,338	5/27/2003	Shaio et al.	
	A166	US	6,581,166	7/17/2003	Hirst et al.	
EXAMINER /Andrew Nalven/				DATE CONSIDERED 11/30/2010		

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)		ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270				
		APPLICANT Victor Larson					
		FILING DATE December 8, 2009	GROUP 3992				
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	
	B100	EP 0 814 589	12/29/97	Harwood et al.		Yes	No
	B101	EP 0 838 930	4/29/98	Alden et al.			
	B102	EP 0 858 189	8/12/98	Maciel et al.			
	B103	DE 199 24 575	12/2/99	Provino et al.			
	B104	GB 2 317 792	4/1/98	Minear et al.			
	B105	GB 2 334 181 A	8/11/99	Noblet			
	B106	EP 836306A1	4/15/98	Sasyan et al.			
	B107	WO 9827783 A	6/25/98	Tello et al.			
	B108	WO 00/17775	3/30/00	Miller et al.			
	B109	WO 01 50688	7/12/01	Kriens			
	B110	WO 98 55930	12/10/98	Tang			
	B111	WO 98 59470	12/30/98	Kanter et al.			
	B112	WO 98/27783	6/25/98	Tello et al.			
	B113	WO 99 38081	7/29/99	Paulsen et al.			
	B114	WO 99 48303	9/23/99	Cox et al.			
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.					
		See sheet Nos. 5-6					
EXAMINER /Andrew Nalven/				DATE CONSIDERED 11/30/2010			

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)		ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270
		APPLICANT Victor Larson	
		FILING DATE December 8, 2009	GROUP 3992
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.	
	C100	Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ssl3/draft302.txt on Feb. 4, 2002, 56 pages.	
	C102	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	C103	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	C104	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	C105	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	C106	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	C107	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	C108	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	C109	Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.	
	C110	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/glossary.html on Feb. 21, 2002, 25 pages.	
	C111	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	C112	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	C113	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	C114	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	C115	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	C116	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
EXAMINER /Andrew Nalven/		DATE CONSIDERED 11/30/2010	

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)		ATTY. DOCKET NO. 077580-0090	SERIAL NO 95/001,270
APPLICANT Victor Larson			
		FILING DATE December 8, 2009	GROUP 3992
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.	
	C117	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	C118	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	C119	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	C120	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	C121	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	C122	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	C123	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	
	C124	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	C125	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	C126	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	C127	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conferece on Communications architectures & protocols. pp. 84-91, ACM Press, NY,NY 1986.	
	C128	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	C129	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	C130	FASBENDER, A. et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	C131	156. Finding Your Way Through the VPN Maze (1999) ("PGP")	
	C132	WatchGuard Technologies, Inc., WatchGuard LiveSecurity for MSS Powerpoint (Feb. 14 2000) (resubmitted)	
	C133	WatchGuard Technologies, Inc., MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes (July 21, 2000)	
EXAMINER /Andrew Nalven/		DATE CONSIDERED 11/30/2010	

*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 1551744-1.068911.0140

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

Reexamination 	Application/Control No. 95/001,270	Applicant(s)/Patent Under Reexamination 7188180
	Certificate Date	Certificate Number

Requester Correspondence Address: <input type="checkbox"/> Patent Owner <input checked="" type="checkbox"/> Third Party
Rothwell, Figg, Renst & Manbeck, P.C. 1425 K Street NW Suite 800 Washington, DC 20005

LITIGATION REVIEW <input checked="" type="checkbox"/>	aln <small>(examiner initials)</small>	1/7/2010 <small>(date)</small>
Case Name		Director Initials
VirnetX et al v. Microsoft - 6:07-cv-00080-LED		<i>Lu Head 4</i> <i>R4</i>

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
1.	
2.	
3.	
4.	



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 03/24/2011
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
03/24/2011	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

MAR 24 2011

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)

NOTICE OF INTENT TO ISSUE INTER PARTES REEXAMINATION CERTIFICATE	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. --

1. Prosecution on the merits is (or remains) closed in this *inter partes* reexamination proceeding. This proceeding is subject to reopening at the initiative of the Office or upon petition. Cf. 37 CFR 1.313(a). A Certificate will be issued in view of:
 - a. The communication filed on _____ by _____.
 - b. Patent owner's failure to file an appropriate timely response to the Office action dated _____.
 - c. The failure to timely file an Appeal with fee by all parties to the reexamination proceeding entitled to do so. 37 CFR 1.959 and 41.61.
 - d. The failure to timely file an Appellant's Brief with fee by all parties to the reexamination proceeding entitled to do so. 37 CFR 41.66(a).
 - e. The decision on appeal by the Board of Patent Appeals and Interferences Court dated _____.
 - f. Other: _____.
2. The Reexamination Certificate will indicate the following:
 - a. Change in the Specification: Yes No
 - b. Change in the Drawings: Yes No
 - c. Status of the Claims:
 - (1) Patent claim(s) confirmed: 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33 and 35.
 - (2) Patent claim(s) amended (including dependent on amended claim(s)): _____
 - (3) Patent claim(s) cancelled: _____.
 - (4) Newly presented claim(s) patentable: _____.
 - (5) Newly presented cancelled claims: _____.
 - (6) Patent claim(s) previously currently disclaimed: _____.
 - (7) Patent claim(s) not subject to reexamination: 2, 3, 5-9, 11, 16, 18, 19, 21-25, 27, 32, 34 and 36-41.
3. Note attached statement of reasons for patentability and/or confirmation.
4. Note attached NOTICE OF REFERENCE CITED, PTO-892.
5. Note attached LIST OF REFERENCES CITED (PTO/SB/08 or PTO/SB/08 substitute).
6. The drawings filed on _____ are are not acceptable.
7. Acknowledgment is made of the claim for priority under 35 U.S.C. § 119(a) - (d) or (f). The certified copy has been received, not been received, been filed in Application/Control No. _____ filed on _____.
8. Note Examiner's Amendment (attachment).
9. Other (attachment).

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.

/Andrew L Nalven/
Primary Examiner, Art Unit 3992

NOTICE OF INTENT TO ISSUE A REEXAMINATION CERTIFICATE

The following action addresses claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of US Patent No. 7,188,180 ("the '180 patent").

An Action Closing Prosecution was issued on June 16, 2010.

A Right of Appeal Notice was issued on December 3, 2010.

Neither party has submitted a notice of appeal.

Status of Claims

Original Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are confirmed.

Rejections Proposed by Requestor – Previously Adopted, Now Not Adopted

1. 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.
2. 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 '180 patent. Specifically, Patent Owner argued that the request and the 1/19/2010 office action did not show that Aventail was published 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

Art Unit: 3992

document's copyright date. The request did not set forth any further evidence of the date of publication.

3. 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.

4. 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*).

5. 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

Art Unit: 3992

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.

6. 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.

7. 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

Art Unit: 3992

conventional domain name service cannot resolve addresses for a secure domain name ('180 patent, column 51 lines 25-35).

8. 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.

9. 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.

10. 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

Art Unit: 3992

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*).

11. 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.

12. 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. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

Art Unit: 3992

13. 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*).

14. 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 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.

Art Unit: 3992

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.

15. 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.

16. 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

Art Unit: 3992

conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

17. 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.

18. 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.

19. 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*

Art Unit: 3992

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*).

20. 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.

21. 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

Art Unit: 3992

by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

22. 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*).

23. 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 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

Art Unit: 3992

'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

24. The non-final action mailed on January 19, 2010 is hereby incorporated by reference.

25. 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.

26. 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.

27. 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.

28. 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 was not adopted for the reasons set forth on Pages 22-23 of the January 19, 2010 non-final office action.

Art Unit: 3992

29. 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.

30. 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 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*) and that a secure domain name service can resolve addresses for a secure domain name whereas a

Art Unit: 3992

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.

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.

Application/Control Number: 95/001,270

Page 15

Art Unit: 3992


Signed:

/Andrew Nalven/

Conferee: ESK

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: HJ

Reexamination 	Application/Control No. 95/001,270	Applicant(s)/Patent Under Reexamination 7188180
	Certificate Date	Certificate Number C1

Requester Correspondence Address: Patent Owner Third Party

Rothwell, Figg, Renst & Manbeck, P.C.
1425 K Street NW
Suite 800
Washington, DC 20005

LITIGATION REVIEW <input checked="" type="checkbox"/>	aln (examiner initials)	1/7/2010 (date)
Case Name		Director Initials
VirnetX et al v. Microsoft - 6:07-cv-00080-LED		<i>Eie Frank to RY</i>

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
1. no concurrent office proceedings	
2. -	
3.	
4.	



UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 2128

SERIAL NUMBER 95/001,270	FILING or 371(c) DATE 12/08/2009 RULE	CLASS 709	GROUP ART UNIT 3992	ATTORNEY DOCKET NO. 077580-0090
------------------------------------	-----------------------------------------------------------	---------------------	-------------------------------	-------------------------------------------

APPLICANTS

7188180, Residence Not Provided;
 VIRNETX INC.(OWNER), SCOTTSVALLEY DRIVE, CA;
 MICROSOFT CORPORATION(3RD. PTY. REQ.), CHEVY CHASE, MD;
 MICROSOFT CORPORATION(REAL PTY. IN INTEREST), CHEVY CHASE, MD;
 ROTHWELL, FIGG, ERNST & MANBECK, P.C., WASHINGTON, DC

**** CONTINUING DATA *******

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

**** FOREIGN APPLICATIONS *******

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Initials				
Verified and Acknowledged <u>/ANDREW L NALVEN/</u> Examiner's Signature					


ADDRESS

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

TITLE

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

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	<input type="checkbox"/> All Fees
		<input type="checkbox"/> 1.16 Fees (Filing)
		<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)
		<input type="checkbox"/> 1.18 Fees (Issue)
		<input type="checkbox"/> Other _____
		<input type="checkbox"/> Credit

Search Notes 	Application/Control No. 95001270	Applicant(s)/Patent Under Reexamination 7188180
	Examiner	Art Unit 3999

SEARCHED			
Class	Subclass	Date	Examiner
709	227		

SEARCH NOTES		
Search Notes	Date	Examiner
Reviewed patented file's prosecution history	1/6/10	aln

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

REEXAMINATION CLERK CHECKLIST

 Ex Parte Reexam *Inter Partes* Reexam

CONTROL NO(S).

9 51001, 2709 19 1

PATENT REEXAMINATION SPECIALIST or REEXAMINATION CLERK:

All of the following items must be completed by you:

A. After completion, the following items should be forwarded (together), via the CRU SPE (for reexams in CRU) or TC SPRE (for reexams in TC), to the Office of Patent Legal Administration. Check box(es) when item is present.

1. This Reexamination Clerk Checklist (PTO-1517)
 2. Examiner Checklist – Reexamination (PTO-1516)
 3. Patent file wrapper (if one exists)

B. Mark the following boxes upon ensuring that the item is present in the file history, in correct form, and complete:

1. The title report, Patent Abstract of Title, or a statement under § 3.73(b)

Filed/Prepared by the Office [Give date & IFW doc code of latest document in IFW]

IFW doc code RXTLRPT Date 12/9/2009

(• - Note Item 26 of Examiner Checklist)

2. All PTO-892 and PTO-1449 reference citation sheets

Total no. of sheets 30 (Note: include only one copy of duplicate sheets)

C. Mark each of the following boxes upon ensuring that the item has been completed by the examiner.

Items on IFW – *Issue Classification* form

1. Patent Number
 2. Reexamination Control Number
 3. International Classification
 4. Original U.S. Classification
 5. Cross References (*Entry present or a dash placed in the x-ref. box for no entry.*)
 6. Assistant Examiner (if any – for reexam in TC)
 7. Primary Examiner
 8. Claim No. for O.G.
 9. Drawing Fig., if any, for certificate and for O.G.
 10. Index of Claims

Items on IFW – *Reexamination* form

11. Co-pending Office Proceedings.
 (information or "No concurrent Office proceedings" entered in lower left hand box)
 12. Reexamination Certificate No. (e.g. C1, C2, C3 to be entered in "Certificate Number" box)
 13. Litigation Review

Items on IFW – *Search Notes* form

14. Reexamination Field of Search ("None" entered, if no search)

• In each of the following items mark either the "YES" or "NO" box.

YES NO

1. Are there any amendments to the description? If yes, identify the IFW doc code(s) and dates of the document(s) containing the amendments. (• - Note Item 1 of Examiner Checklist).

IFW doc code _____ Date / /
IFW doc code _____ Date / /
IFW doc code _____ Date / /

2. Are there any changes to the patent drawings? If yes, identify the following. (• - Note Item 2 of Examiner Checklist).

IFW doc code _____ Date / /
Fig. No(s). containing changes: _____

IFW doc code _____ Date / /
Fig. No(s). containing changes: _____

3. Was a terminal disclaimer filed DURING reexamination and approved? (• - Note Item 3 of Examiner Checklist.) If yes, the Terminal Disclaimer "approved" box on the IFW - *Terminal Disclaimer* form must be checked. Also, indicate the document(s) containing the terminal disclaimer(s).

IFW doc code _____ Date / /
IFW doc code _____ Date / /

4. Have any certificates of correction been issued? If yes, indicate date(s) issued. (• - Note Item 4 of Examiner Checklist.)

_____ Aug 7, 2007 _____

5. Has any document been submitted indicating the names of registered attorneys or agents or a law firm to be published on the reexam certificate? If yes, indicate the filing date and IFW doc code of the document containing the names. (• - Note Item 5 of Examiner Checklist.)

Filed [Give filing date(s) & IFW doc code(s)] _____

6. Was/were any statutory disclaimers or dedications filed prior to, or during, the reexamination, and approved? If yes, complete the following, *and* place copy of approved dedication/statutory disclaimer in reexamination file. (• - Note Items 9 & 10 of the Examiner Checklist.)

1a. Filed - IFW doc code _____ Date / /
1b. O.G. citation _____
1c. Claims disclaimed/dedicated _____

2a. Filed - IFW doc code _____ Date / /
2b. O.G. citation _____
2c. Claims disclaimed/dedicated _____

YES NO

7. Have any claims been amended? A claim is "amended" if there is any change to its text. If yes, list all amended claims by the most recent IFW doc code date of the document which contains the final version of all of the amended claims. (* - Note Item 12 of Examiner Checklist.)

IFW doc code _____ Date ____ / ____ / ____
Claims _____
IFW doc code _____ Date ____ / ____ / ____
Claims _____
IFW doc code _____ Date ____ / ____ / ____
Claims _____
IFW doc code _____ Date ____ / ____ / ____
Claims _____

(Note: these claims will be printed on the reexamination certificate.)

8. Have new claims been added and allowed during the reexamination? If yes, (1) indicate the filing date and IFW doc code of the document containing the final version of the allowed, new claims and (2) list the claims by final number. (* - Note Item 14 of Examiner Checklist.)

IFW doc code _____ Date ____ / ____ / ____
Claims _____
IFW doc code _____ Date ____ / ____ / ____
Claims _____
IFW doc code _____ Date ____ / ____ / ____
Claims _____
IFW doc code _____ Date ____ / ____ / ____
Claims _____

(Note: these claims will be printed on the reexamination certificate.)

E. Have any of the following items been changed or added since the patent was issued? If yes, indicate the filing date and IFW doc code of the document containing the change/addition and mark the appropriate boxes upon ensuring statement is correct. Certificate of Correction changes are not to be indicated here; instead see Item D.4.

YES NO INID CODE

(54) 1. Title of Invention. (* - Note Item 21 of Examiner Checklist.)

IFW doc code _____ Date ____ / ____ / ____

Update information has been entered on bib data sheet.

(75) 2. Inventor(s). (* - Note Item 22 of Examiner Checklist.)
or
 (76)

IFW doc code _____ Date ____ / ____ / ____

(73) 3. Assignee (if any): Compare assignee information on (a) title report, Patent Abstract of Title, or 37 CFR 3.73(b) statement (see Item B1 above), with (b) printed patent entry, and (c) reexamination bib data sheet entry. Assignment/owner document:

IFW doc code _____ Date ____ / ____ / ____

Update information has been entered on reexamination bib data sheet.

YES NO INID
CODE

4. Continuing Data. (• • - Note Item 23 of Examiner Checklist.)

(60) a. --Combination of Division and Continuation and/or C.I.P.

Document adding data:

IFW doc code _____ Date ____ / ____ / ____

-- Provisional Application(s)

Document adding data:

IFW doc code _____ Date ____ / ____ / ____

(62) b. Division(s).

Document adding data:

IFW doc code _____ Date ____ / ____ / ____

(63) c. Continuation(s) and/or C.I.P.

Document adding data:

IFW doc code _____ Date ____ / ____ / ____

(64) d. Reissue(s) where patent reissues during pendency of reexam.

Amendment document containing the statement "This is a reissue of _____."-

IFW doc code _____ Date ____ / ____ / ____

Update information has been entered on reexamination bib data sheet.

Update information has been entered in the first sentence of the specification following the title. 37 CFR 1.78(a).

(30) 5. Foreign Priority. (• • - Note Item 24 of Examiner Checklist.)

Document adding data:

IFW doc code _____ Date ____ / ____ / ____

Update information has been entered on reexamination bib data sheet.

(57) 6. Abstract. (• • - Note Item 25 of Examiner Checklist.)

IFW doc code _____ Date ____ / ____ / ____

Patent Reexamination Specialist

DATE

CRU SPEC SPRE REVIEW

DATE

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 03/29/2011

AMULLINS SALE #00000002 Mailroom Dt: 03/28/2011 500412 95001270
01 FC : 8012 15.00 DA



US007188180C1

(12) **INTER PARTES REEXAMINATION CERTIFICATE** (0274th)

United States Patent

(10) **Number:** **US 7,188,180 C1**

Larson et al.

(45) **Certificate Issued:** **Jun. 7, 2011**

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

4,933,846 A 6/1990 Humphrey et al.
4,988,990 A 1/1991 Warrior
5,276,735 A 1/1994 Boebert et al.
5,303,302 A 4/1994 Burrows

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

(Continued)

(73) **Assignee:** **Virnetx Inc.**, Scotts Valley Drive, CA (US)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999
EP 0 814 589 12/1997
EP 836306 A1 4/1998
EP 0 838 930 4/1998
EP 0 858 189 8/1998

Reexamination Request:

No. 95/001,270, Dec. 8, 2009

(Continued)

Reexamination Certificate for:

Patent No.: **7,188,180**
Issued: **Mar. 6, 2007**
Appl. No.: **10/702,486**
Filed: **Nov. 7, 2003**

OTHER PUBLICATIONS

Exhibit 2 "Aventail Connect v.3.1/v2.6 Administrator's Guide", pp. 1-120, 1996-1999.

Exhibit 3, "Windows NT Server, Virtual Private Network: An Overview", pp. 1-28, 1998.

Exhibit 4, "Network Working Group Request For Comments 1035", pp. 1-56, 1987.

Certificate of Correction issued Aug. 7, 2007.

Related U.S. Application Data

(Continued)

(60) Division of application No. 09/558,209, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/227; 709/228**

(58) **Field of Classification Search** **709/227**
See application file for complete search history.

Primary Examiner—Andrew L Nalven

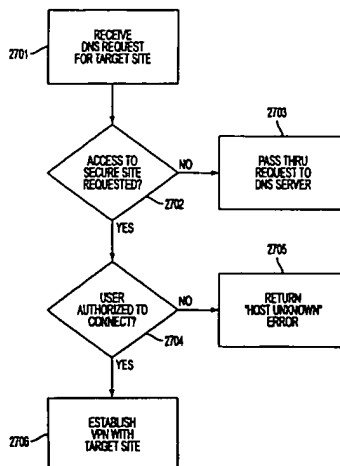
(57) **ABSTRACT**

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

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502 A 7/1959 Roper et al.



WO	WO 98/27783	6/1998
WO	WO 98 55930	12/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/17775	3/2000
WO	WO 0017775	3/2000
WO	WO 00/70458	11/2000
WO	WO 01/16766	3/2001
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Exhibit 5, "Kusur" Building and Managing Virtual Private Networks, pp. 1-396, 1998.

Exhibit 6, "Kaufman et al.," Implementing IPsec, pp. 1-280, 1999.

Exhibit 7, "James Galvin" Public Key Distribution Secure DNS, pp. 1-12, 1996.

Exhibit 8A, Gauntlet Firewall for Windows NT Administrator's Guide, pp. 1-137, 1998-1999.

Exhibit 8B, Gauntlet Firewall for windows NT Administrator's Guide, pp. 138-275, 1998-1999.

Exhibit 9, "Windows NT Technical Support: Hands On, Self Paced Training for Supporting Version 4.0", pp. 1-106, 1998.

Exhibit 10, Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, pp. 1-30, 1997.

Exhibit 11, Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources, pp. 1-216, 2000.

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).

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

Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from <http://www.netscape.com/eng/ss13/draft302.txt> on Feb. 4, 2002, 56 pages.

August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.

D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.

D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.

Davila J et al. "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666.

Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.

Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", Internet Draft, Apr. 1998, pp. 1-51.

F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.

Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/glossary.html on Feb. 21, 2002, 25 pages.

J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.

James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.

Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.

Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.

Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.

P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.

RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP).

RFC 2543-SIP (dated Mar. 1999); Session Initiation Protocol (SIP or SIPS).

Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.

Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.

Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.

Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.

Search Report, IPER (dated Feb. 6, 2002), International Application no. PCT/US01/13261.

Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.

Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conference on Communications architecture & protocols. pp. 84-91, ACM Press, NY,NY 1986.

Shree Murthy et al., "Congestion-Oriented Shortest Multipath Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.

W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.

Fasbender, A. et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.

156. Finding Your Way Through the VPN Maze (1999) ("PGP").

WatchGuard Technologies, Inc., WatchGuard LiveSecurity for MSS Powerpoint (Feb. 14, 2000) (resubmitted).

WatchGuard Technologies, Inc., MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes (Jul. 21, 2000).

U.S. Appl. No. 60/134,547, filed May 17, 1999, Victor Sheymov.

U.S. Appl. No. 60/151,563, filed Aug. 31, 1999, Bryan Whittles.

- U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.
- Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, *VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation*.
- Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.
- Concordance Table For the References Cited in Tables on pp. 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.
- I. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (Apr. 1989) (RFC1101, DNS SRV).
- DNS-related correspondence dated Sep. 7, 1993 to Sep. 20, 1993. (Pre KX, KX Records).
- R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (Aug. 3, 1993). (Atkinson NRL, KX Records).
- Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96).
- Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology).
- "Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (Mar. 1996). (Safe Surfing, Website Art).
- Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing).
- "IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, <http://www.sandleman.ca/ipsec/1996/08/msg00018.html> (Jun. 1996). (IPSec Minutes, FreeS/WAN).
- J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, Jul. 1996. (Galvin, DNSSEC).
- J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPsec Working Group Mailing List Archives (Aug. 1996). (Gilmore DNS, FreeS/WAN).
- H. Orman, et al. "Re: 'Re: DNS?0 was Re: Key Management, anyone?'" IETF IPsec working Group Mailing List Archive (Aug. 1996-Sep. 1996). (Orman DNS, FreeS/WAN).
- Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (Oct. 1996). (RFC 2052, DNS SRV).
- Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (Nov. 18, 1996). (SSL, Underlying Security Technology).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 2, 1996). (RFC 2543 Internet Draft 1).
- 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).
- Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista).
- Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX).
- Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX).
- Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," available at <http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html> (1997). (AutoSOCKS, Aventail).
- Aventail Corp. "Aventail VPN Data Sheet," available at <http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html> (1997). (Data Sheet, Aventail).
- Aventail Corp., "Directed VPN Vs. Tunnel," available at <http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html> (1997). (Directed VPN, Aventail).
- 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).
- Aventail Corp., "Socks Version 5," Aventail Whitepaper, available at <http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/socks5wp.html> (1997). (Socks, Aventail).
- Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail).
- Goldschlag, et al. "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing).
- Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology).
- Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1989 PDC DVD-ROM). (IP Security, Microsoft prior Art VPN Technology).
- Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology).
- Microsoft Corp., *Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM). (Routing, Microsoft Prior Art VPN Technology).
- Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology).
- J. Mark Smith et al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista).
- Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IP Security*, <draft-ietf-ipsec-vpn-00.txt> (Mar. 12, 1997). (Doraswamy).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Mar. 27, 1997). (RFC 2543 Internet Draft 2).
- Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, Apr. 3, 1997. (Secure Authentication, Aventail).
- D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (Apr. 15, 1997). (Analysis, Underlying Security Technologies).

- 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).
- 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).
- Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," Jun. 2, 1997. (First VPN, Aventail).
- Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High Assurance Computer Systems (Jun. 2, 1997). (Syverson, Onion Routing).
- Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIG Telecommunications Project Team and Bellcore (Jun. 16, 1997), (AIAG Requirements, ANX).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 31, 1997). (RFC 2543 Internet Draft 3).
- R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (Nov. 1997). (RFC 2230, KX Records).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 11, 1997). (RFC 2543 Internet Draft 4).
- 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).
- Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology).
- Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at <http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue>). (NT Beta, Microsoft Prior Art VPN Technology).
- "What ports does SSL use" available at stason.org/TU-LARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV).
- Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, Jan. 19, 1998. (VPN V2.6, Aventail).
- R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, Feb. 6, 1998. (Moskowitz).
- H. Schulzrinne, et al., "Internet Telephony Gateway Location," Proceedings of IEEE Infocom '98. The Conference on Computer Communications, vol. 2 (Mar. 29-Apr. 2, 1998). (Gateway, Schulzrinne).
- C. Huitema, et al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP).
- DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (May 14, 1998). (RFC 2543 Internet Draft 5).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jun. 17, 1998). (RFC 2543 Internet Draft 6).
- D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (Jul. 1998). (RFC 2367).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 16, 1998). (RFC 2543 Internet Draft 7).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Aug. 7, 1998). (RFC 2543 Internet Draft 8).
- Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (Aug. 18, 1998). (Focus, Microsoft Prior Art VPN Technology).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Sep. 18, 1998). (RFC 2543 Internet Draft 9).
- Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (Nov. 1998). (RFC 2401, Underlying Security Technologies).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 12, 1998). (RFC 2543 Internet Draft 10) 9.
- Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (Dec. 1998). (DNS-SEC-7).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft. (Dec. 15, 1998). (RFC 2543 Internet Draft 11).
- Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide." (1999). (Aventail Administrator 3.1, Aventail).
- Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide" (1999). (Aventail User 3.1, Aventail).
- Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail).
- Kaufman et al. "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN References).
- Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, Underlying Security Technologies).
- Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW).
- Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*. <draft-ietf-dnsind-frc2052bis-02.txt> (Jan. 1999). (Gulbrandsen 99, DNS SRV).
- C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs).
- M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jan. 15, 1999). (RFC 2543 Internet Draft 12).
- Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (Jan. 28, 1999). (Goldschlag III, Onion Routing).
- H. Schulzrinne, "Internet Telephony: architecture and protocols—an IETF perspective," *Computer Networks*, vol. 31, No. 3 (Feb. 1999). (Telephony, Schulzrinne).
- M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (Dec. 1996-Mar. 1999). (Handley, RFC 2543).
- FreeS/WAN Project, *Linus FreeS/WAN Compatibility Guide* (Mar. 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN).

- Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX).
- Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (Jun. 21, 1999). (Hornstein, DNS SRV).
- Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPsec Based Virtual Private Networks (VPNs)", IETF Internet Draft (Oct. 1999). (Bhattacharya LDAP VPN).
- B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (Oct. 15, 1999). (Patel).
- Goncalves, et al. *check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW).
- "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan. 2000). (FirstVPN Microsoft).
- Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (Feb. 2000). (RFC 2782, DNS SRV).
- Mitre Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (Feb. 2000). (MITRE SIPRNET).
- H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," *Mobile Computing and Communications Review*, vol. 4, No. 3, pp. 47-57 (Jul. 2000). (Application, SIP).
- Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (Jun. 2001). (DARPA, VPN Systems).
- ANX 101: Basic ANX Service Outline. (Outline, ANX).
- ANX 201: Advanced ANX Service. (Advanced, ANX).
- Appendix A: Certificate Profile for ANS IPsec Certificates. (Appendix, ANX).
- Assured Digital Products. (Assured Digital).
- Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail).
- Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET).
- Data Fellows F-Secure VPN+ (F-Secure VPN+).
- Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution (RASP, SIPRNET).
- Onion Routing*, "Investigation of Route Selection Algorithms," available at <http://www.onion-router.net/Archives/Route/index.html>. (Route Selection, Onion Routing).
- Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure SIPRNET).
- Sparta "Dynamic Virtual Private Network." (Sparta, VPN Systems).
- Standard Operation Procedure for Using the 1910 Secure Modems. (Standard SIPRNET).
- Publicly available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN).
- Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec).
- Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide—Unix, Firewall Products).
- Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide—NT, Firewall Products).
- Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products).
- Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (Mar. 19, 1999) (Gauntlet Unix Release Notes, Firewall Products).
- Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products).
- Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products).
- Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN).
- Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN).
- Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN).
- Darrel Kindred *Dynamic Virtual Private Networks (DVPN)* (Dec. 21, 1999) (Kindred DVPN, DVPN).
- Dan Sterne et. al. *TIS Dynamic Security Perimeter Research Project Demonstration* (Mar. 9, 1998) (Dynamic Security Perimeter, DVPN).
- Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (Jan. 5, 2000) (Kindred DVPN Capability, DVPN) 11.
- Oct. 7, and 28, 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN).
- James Just & Dan Sterne *Security Quickstart Task Update* (Feb. 5, 1997) (Security Quickstart, DVPN).
- Virtual Private Network Demonstration dated Mar. 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN).
- GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (Mar. 10, 1998) (IFD 1.1, DVPN).
- Microsoft Corp. Windows NT Server Product Documentation: Administration Guide—Connection Point Services, available at <http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.msp> (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.).
- Microsoft Corp. windows NT Server Product Documentation: Administration Kit Guide—Connection Manager, available at <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.).
- Microsoft Corp. Autodial Heuristics, available at <http://support.microsoft.com/kb/164249> (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.).

- Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) available at [http://msdn2.microsoft.com/en-us/library/ms809332\(printer\).aspx](http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx) (Cariplo I).
- Marc Levy, COM Internet Services (Apr. 23, 1999), available at [http://msdn2.microsoft.com/en-us/library/ms809302\(printer\).aspx](http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx) (Levy).
- Markus Horstmann and Mary Kirtland, DCOM Architecture (Jul. 23, 1997), available at [http://msdn2.microsoft.com/en-us/library/ms809311\(printer\).aspx](http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx) (Horstmann).
- Microsoft Corp., DCOM: A Business Overview (Apr. 1997), available at [http://msdn2.microsoft.com/en-us/library/ms809320\(printer\).aspx](http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx) (DCOM Business Overview I).
- Microsoft Corp., DCOM Technical Overview (Nov. 1996), available at [http://msdn2.microsoft.com/en-us/library/ms809340\(printer\).aspx](http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx) (DCOM Technical Overview I).
- Microsoft Corp., DCOM Architecture White Paper (1998) available in PDC DVD-ROM (DCOM Architecture).
- Microsoft Corp. DCOM—The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) available in PDC DVD-ROM (DCOM Business Overview II).
- Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) available in PDC DVD-ROM (Cariplo II).
- Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) available in PDC DVD-ROM (DCOM Solutions in Action).
- Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) available 12 in PDC DVD-ROM (DCOM Technical Overview II).
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](http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx) (Suhy).
126. Aaron Skonnard, *Essential WinInet* 313–423 (Addison Wesley Longman 1998) (Essential WinInet).
- Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) available at [http://msdn2.microsoft.com/enus/library/ms811078\(printer\).aspx](http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx) (Using PPTP).
- Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, <http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspix> (Internet Connection Services I).
- Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, available at <http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgsttrc.mspix> (Internet Connection Services II).
- 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.mspix> (IE5 Corporate Development).
- Mark Minasi, *Mastering Windows NT Server 4* 1359–1442 (6th ed., Jan. 15, 1999) (Mastering Windows NT Server).
- Hands On, Self-Paced Training for Supporting Version 4.0* 371–473 (Microsoft Press 1998) (Hands On).
- Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), available at <http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspix> (MS PPTP).
- Kenneth Gregg, et al., *Microsoft Windows NT Server Administrator's Bible* 173–206, 883–911, 974–1076 (IDG Books Worldwide 1999) (Gregg).
- Microsoft Corp., Remote Access (Windows), available at [http://msdn2.microsoft.com/en-us/library/bb545687\(VS.85,printer\).aspx](http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx) (Remote Access).
- Microsoft Corp., Understanding PPTP (Windows NT 4.0), available at <http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspix> (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.)
- Microsoft Corp., Windows NT 4.0: Virtual Private Networking, available at <http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspix> (NT4VPN) (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.)
- Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299–399 (IDG Books Worldwide 1998) (Network Plumbing).
- 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/rrascho01.mspix> (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.
- 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.mspix> (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.)
- F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3).
- F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3).
- F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3).
- F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3).
- F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3).
- F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3).
- F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6).
- F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6).
- F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6).
- F-Secure, *F-Secure Evaluation Kit* (Sep. 1998) (FSECURE 00000009) (Evaluation Kit 9).
- F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sep. 1998) (from FSECURE 00000009) (SSH Guide 9).
- F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sep. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9).
- F-Secure, *F-Secure VPN+* (Sep. 1998) (from FSECURE 00000009) (VPN+ Guide 9).

- F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools).
- F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide).
- SafeNet, Inc., *VPN Policy Manager* (Jan. 2000) (VPN Policy Manager).
- F-Secure, *F-Secure VPN+ for Windows NT 4.0* (1998) (from FSECURE 00000009) (FSecure VPN+).
- IRE, Inc., *SafeNet/Soft-PK Version 4* (Mar. 28, 2000) (Soft-PK Version 4).
- IRE/SafeNet Inc., *VPN Technologies Overview* (Mar. 28, 2000) (Safenet VPN Overview).
- IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (Jun. 22, 1999) (Safenet Addendum).
- IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (Mar. 30, 2000) (VPN Policy Manager System Description).
- IRE, Inc., *About SafeNet / VPN Policy Manager* (1999) (About Safenet VPN Policy Manager).
- IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager).
- Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (Jul. 22, 1996) (Gauntlet Functional Summary).
- Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall).
- Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79.
- Todd W. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers).
- Bernard Aboba et al., *Securing L2TP using IPSEC* (Feb. 2, 1999).
156. *Finding Your Way Through the VPN Maze* (1999) ("PGP").
- Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview).
- TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep").
- WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000).
- Watchguard Technologies, Inc., *MSS Firewall Specifications* (1999).
- WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000).
- WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (Feb. 2000).
- WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14, 2000).
- WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes* (Jul. 21, 2000).
- Air Force Researach Laboratory, *Statement of Work for Information Assurance System Architecture and Integration*, PR No. N-8-6106 (Contract No. F30602-98-C-0012) (Jan. 29, 1998).
- GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (Sep. 21, 1998).
- BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (Mar. 16-Apr. 30, 1998).
- DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*.
- GTE Internetworking, *Contractor's Program Progress Report* (Mar. 16-Apr. 30, 1998).
- Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (Jan. 30, 2001).
- Virtual Private Networking Countermeasure Characterization* (Mar. 30, 2000).
- Virtual Private Network Demonstration* (Mar. 21, 1998).
- Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000).
- Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000).
- NAI Labs, *IFE 3.1 Integration Demo* (2000).
- Information Assurance, *Science Fair Agenda* (2000).
- Darrell Kindred et al., *Proposed Threads for IFE 3.1* (Jan. 13, 2000).
- IFE 3.1 Technology Dependencies* (2000).
- IFE 3.1 Topology* (Feb. 9, 2000).
- Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (Jan. 10-11, 2000).
- Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000).
- Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v. 2* (2000).
- Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v. 3* (2000).
- T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (Aug. 1, 1999) (VPNA).
- Network Associates Products—PGP Total Network Security Suite, *Dynamic Virtual Private Networks* (1999).
- Microsoft Corporation, *Microsoft Proxy Server 2.0* (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology).
- David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology).
- Microsoft Corporation, *Setting Server Parameters* (1997 copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Micorsoft Prior Art VPN Technology).
- Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology).
- Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology).
- M. Shane Stigler & Mark A. Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology).
- David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology).
- John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology).
- Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN).
- Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN).
- File History for U.S. Appl. No. 09/653,201, Applicant(s): Whittle Bryan, et al., filed Aug. 31, 2000.
- AutoSOCKS v2.1*, Datasheet, <http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html>.

- Ran Atkinson, *Use of DNS to Distribute Keys*, Sep. 7, 1993, <http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html>.
- FirstVPN Enterprise Networks, Overview.
- Chapter 1: Introduction to Firewall Technology, Administration Guide; Dec. 19, 2007, http://www.books24x7.com/bookid_762/viewer_r.asp?book/id=762&chunked=41065062.
- The TLS Protocol Version 1.0; Jan. 1999; p. 65 of 71.
- Elizabeth D. Zwicky, et al., *Building Internet Firewalls*, 2nd Ed.
- Virtual Private Networks—Assured Digital Incorporated—ADI 4500; <http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm>.
- Accessware—The Third Wave in Network Security, Conclave from Internet Dynamics; <http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html>.
- Extended System Press Release, Sep. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com.
- Socks Version 5; Executive Summary; <http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html>.
- Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sep. 15, 1997; <http://web.archive.org/web/19980210014150/interdyn.com>.
- Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing.
- Microsoft Corporation's Fifth Amended Invalidity Contentions dated Sep. 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.
- The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (Nov. 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (Nov. 1989); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- Douglas Maughan, et al., "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.
- Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (Nov. 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (Jul. 1996) ("Galvin").
- David Kosiur, "Building and Managing Virtual Private Networks" (1998).
- P. Mockapetris, "Domain Names—Implementation and Specification," Network Working Group, RFC 1035 (Nov. 1987).
- Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.

1
INTER PARTES
REEXAMINATION CERTIFICATE
ISSUED UNDER 35 U.S.C. 316

NO AMENDMENTS HAVE BEEN MADE TO
THE PATENT

2
AS A RESULT OF REEXAMINATION, IT HAS BEEN
DETERMINED THAT:

The patentability of claims 1, 4, 10, 12-15, 17, 20, 26,
28-31, 33 and 35 is confirmed.

5 Claims 2, 3, 5-9, 11, 16, 18, 19, 21-25, 27, 32, 34 and
36-41 were not reexamined.

* * * * *