Subst. for form 1449/PTO

Complete if Known 13339257 - GAU: 2453

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

O.I.P.E. IAP3 MAR 0 9 2012 PATENT & TRADEMARK OFFICE

Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Patent Date	Inventor	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	2,895,502	07/21/1959	Roper et al.	
	A3	4,761,334	08/1988	Sagoi et al.	
	A4	4,885,778	12/5/1989	Weiss, Kenneth	
	A5	4,920,484	4/24/1990	Ranade	
	A6	4,933,846	06/12/1990	Humphrey et al.	
	A7	4,952,930	08/28/1990	Franaszek et al.	
	A8	4,988,990	01/29/1991	Warrior	
	A9	5,164,988	11/17/1992	Matyas	
	A10	5,204,961	04/20/1993	Barlow	
	A11	5,276,735	01/04/1994	Boebert et al	
	A12	5,303,302	04/12/1994	Burrows	
	A13	5,311,593	05/10/1994	Carmi	
	A14	5,329,521	07/12/1994	Walsh et al.	
	A15	5,341,426	08/23/1994	Barney et al.	
	A16	5,367,643	11/22/1994	Chang et al	
	A17	5,384,848	01/24/1995	Kikuchi	
	A18	5,511,122	04/23/1996	Atkinson	
	A19	5,548,646	08/20/1996	Aziz et al.	
	A20	5,559,883	09/24/1996	Williams	
	A21	5,561,669	10/01/1996	Lenney et al	
	A22	5,588,060	12/24/1996	Aziz	
	A23	5,590,285	12/31/1996	Krause et al.	
	A24	5,625,626	04/29/1997	Umekita	
	A25	5,629,984	05/13/1997	McManis	
	A26	5,654,695	08/05/1997	Olnowich et al	
	A27	5,682,480	10/28/1997	Nakagawa	
	A28	5,689,566	11/18/1997	Nguyen	
	A29	5,689,641	11/18/1997	Ludwig et al.	
	A30	5,740,375	04/14/1998	Dunne et al.	
	A31	5,757,925	05/1998	Faybishenko	
	A32	5,764,906	06/1998	Edelstein et al.	
	A33	5,771,239	06/23/1998	Moroney et al.	
	A34	5,774,660	6/30/1998	Brendel et al	
	A35	5,787,172	07/28/1998	Arnold	
	A36	5,790,548	08/04/1998	Sitaraman et al.	
	A37	5,796,942	08/18/1998	Esbensen	
	A38	5,805,801	09/08/1998	Holloway et al.	
	A39	5,805,803	09/08/1998	Birrell et al.	
	A40	5,822,434	10/13/1998	Caronni et al.	
	A41	5,842,040	11/24/1998	Hughes et al.	
	A42	5,845,091	12/01/1998	Dunne et al.	
	A43	5,864,666	01/1999	Shrader, Theodore Jack London	
	A44	5,867,650	02/02/1998	Osterman	
	A45	5,870,610	02/09/1999	Beyda et al.	
	A46	5,878,231	05/02/1999	Baehr et al	
	A47	5,892,903	04/06/1999	Klaus	
	A48	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A49	5,905,859	05/18/1999	Holloway et al.	
	A50	5,918,018	06/29/1999	Gooderum et al.	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	A51		5,918,019	06/29/1999	Valencia	
	A52		5,950,195	09/07/1999	Stockwell et al.	
	A53		5,950,519	09/14/1999	Anatoli	
	A54		5,960,204	09/28/1999	Yinger et al.	
	A55		5,996,016	11/30/1999	Thalheimer et al.	
	A56		6,006,259	12/21/1999	Adelman et al.	
	A57		6,006,272	12/21/1999	Aravamudan et al	
	A58		6,016,318	01/18/2000	Tomoike	
	A59		6,016,512	01/18/2000	Huitema	
	A60		6,041,342	03/21/2000	Yamaguchi	
	A61		6,052,788	04/2000	Wesinger et al.	
	A62		6,055,574	04/25/2000	Smorodinsky et al.	
	A63		6,061,346	05/2000	Nordman, Mikael	
	A64		6,061,736	05/09/2000	Rochberger et al	
	A65		6,079,020	06/20/2000	Liu	
	A66		6,081,900	06/2000	Subramaniam et al.	
	A67		6,092,200	07/18/2000	Muniyappa et al.	
	A68		6,101,182	08/2000	Sistanizadeh et al.	
	A69		6,119,171	09/12/2000	Alkhatib	
	A70		6,119,234	09/12/2000	Aziz et al.	
	A71		6,147,976	11/14/2000	Shand et al.	
	A72		6,157,957	12/05/2000	Berthaud	
	A73		6,158,011	12/05/2000	Chen et al.	
	A74		6,168,409	01/02/2001	Fare	
	A75		6,173,399	01/09/2001	Gilbrech	
	A76		6,175,867	01/16/2001	Taghadoss	
	A77		6,178,409	01/23/2001	Weber et al.	
	A78		6,178,505	01/23/2001	Schneider et al	
	A79		6,179,102	01/30/2001	Weber, et al.	
	A80		6,182,141	1/30/2001	Blum et al.	
	A81		6,199,112	03/2001	Wilson, Stephen K.	
	A82		6,202,081	03/2001	Naudus, Stanley T.	
	A83		6,222,842	04/24/2001	Sasyan et al.	
	A84		6,223,287	04/24/2001	Douglas et al.	
	A85		6,226,748	05/01/2001	Bots et al.	
	A86		6,226,751	05/01/2001	Arrow et al..	
	A87		6,233,618	05/15/2001	Shannon	
	A88		6,243,360	06/05/2001	Basilico	
	A89		6,243,749	06/05/2001	Sitaraman et al.	
	A90		6,243,754	06/05/2001	Guerin et al	
	A91		6,246,670	06/12/2001	Karlsson et al.	
	A92		6,256,671	07/03/2001	Strentzsch et al.	
	A93		6,262,987	07/17/01	Mogul, Jeffrey C.	
	A94		6,263,445	07/17/2001	Blumenau	
	A95		6,269,099	07/31/2001	Borella et al.	
	A96		6,286,047	09/04/2001	Ramanathan et al	
	A97		6,298,341	10/02/01	Mann, et al.	
	A98		6,301,223	10/9/2001	Hrastar et al	
	A99		6,308,213	10/23/2001	Valencia	
	A100		6,308,274	10/23/2001	Swift	
	A101		6,311,207	10/30/2001	Mighdoll et al	
	A102		6,314,463	11/2001	Abbott et al.	
	A103		6,324,161	11/27/2001	Kirch	
	A104		6,330,562	12/11/2001	Boden et al.	
	A105		6,332,158	12/18/2001	Risley et al.	
	A106		6,333,272	12/25/01	McMillin, et al.	
	A107		6,338,082	01/08/02	Schneider, Eric	

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

/Krisna Lim/ 07/10/2013

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	A108		6,353,614	03/05/2002	Borella et al.	
	A109		6,425,003	07/23/2002	Herzog et al.	
	A110		6,430,155	08/06/2002	Davie et al	
	A111		6,430,610	08/06/2002	Carter	
	A112		6,487,598	11/26/2002	Valencia	
	A113		6,496,867	12/17/2002	Beser et al.	
	A114		6,502,135	12/2002	Munger et al.	
	A115		6,505,232	01/07/2003	Mighdoll et al	
	A116		6,510,154	01/21/2003	Mayes et al	
	A117		6,549,516	04/15/2003	Albert et al	
	A118		6,557,037	04/2003	Provino, Joseph E.	
	A119		6,560,634	05/06/2003	Broadhurst	
	A120		6,571,296	05/27/2002	Dillon	
	A121		6,571,338	05/27/2003	Shaio et al.	
	A122		6,581,166	7/17/2003	Hirst et al.	
	A123		6,606,708	08/12/2003	Devine et al.	
	A124		6,615,357	9/2/2003	Boden et al.	
	A125		6,618,761	09/09/2003	Munger et al.	
	A126		6,671,702	12/30/2003	Kruglikov et al	
	A127		6,687,551	2/3/2004	Steindl	
	A128		6,687,746	02/03/04	Shuster, et al.	
	A129		6,701,437	03/02/2004	Hoke et al.	
	A130		6,714,970	3/30/2004	Fiveash et al.	
	A131		6,717,949	4/6/2004	Boden et al.	
	A132		6,751,738	06/15/2004	Wesinger, Jr. et al..	
	A133		6,752,166	06/22/04	Lull, et al.	
	A134		6,757,740	06/29/04	Parekh, et al.	
	A135		6,760,766	7/6/2004	Sahlqvist	
	A136		6,813,777	11/2004	Weinberger et al.	
	A137		6,826,616	11/30/2004	Larson et al.	
	A138		6,839,759	1/4/2005	Larson et al.	
	A139		6,937,597	08/30/2005	Rosenberg et al.	
	A140		60/134,547	05/17/1999	Victory Sheymov	
	A141		60/151,563	08/31/1999	Bryan Whittles	
	A142		7,010,604	3/7/2006	Munger et al.	
	A143		7,039,713	05/2006	Van Gunter et al.	
	A144		7,072,964	07/04/2006	Whittle et al.	
	A145		7,133,930	11/7/2006	Munger et al.	
	A146		7,167,904	01/23/07	Devarajan, et al.	
	A147		7,188,175	03/06/07	McKeeth, James A.	
	A148		7,188,180	3/6/2007	Larson et al.	
	A149		7,197,563	3/27/2007	Sheymov et al.	
	A150		7,353,841	04/08/08	Kono, et al.	
	A151		7,418,504	08/2008	Larson et al.	
	A152		7,461,334	12/02/08	Lu, et al.	
	A153		7,490,151	02/2009	Munger et al.	
	A154		7,493,403	02/2009	Shull et al.	
	A155		7,584,500	09/2009	Dillon et al.	
	A156		7,764,231	07/27/2010	Karr et al.	
	A157		7,852,861	12/2010	Wu et al.	
	A158		7,921,211	04/2011	Larson et al.	
	A159		7,933,990	04/2011	Munger et al.	
	A160		8,051,181	11/2011	Larson et al.	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2002/0004898	1/10/02	Droge	
	B3	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
	B4	US2004/0199493	10/2004	Ruiz et al.	
	B5	US2004/0199520	10/2004	Ruiz et al.	
	B6	US2004/0199608	10/2004	Rechterman et al.	
	B7	US2004/0199620	10/2004	Ruiz et al.	
	B8	US2005/0055306	3/10/05	Miller et al.	
	B9	US2005/0108517	05/2005	Dillon et al.	
	B10	US2006/0059337	03/16/2006	Polyhonen et al.	
	B11	US2006/0123134	06/2006	Munger et al.	
	B12	US2007/0208869	09/2007	Adelman et al.	
	B13	US2007/0214284	09/2007	King et al.	
	B14	US2007/0266141	11/2007	Norton, Michael Anthony	
	B15	US2008/0005792	01/2008	*Larson et al.	
	B16	US2008/0144625	06/2008	Wu et al.	
	B17	US2008/0235507	09/2008	Ishikawa et al.	
	B18	US2009/0193498	07/2009	Agarwal et al.	
	B19	US2009/0193513	07/2009	Agarwal et al.	
	B20	US2009/0199258	08/2009	Deng et al.	
	B21	US2009/0199285	09/2009	Agarwal et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 – Number 4 –Kind Code5 *(if known)*	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	C1	DE19924575	12/2/99	Provino et al.			
	C2	EP0814589	12/29/1997	AT&T Corp.			
	C3	EP0838930	4/29/1988	Digital Equipment Corporation			
	C4	EP0858189	8/12/98	Maciel et al.			
	C5	EP836306	4/15/1998	HEWLETT PACKARD CO			
	C6	GB2317792	04/01/1998	Secure Computing Corporation			
	C7	GB2334181	08/11/1999	NEC Technologies			
	C8	GB2340702	02/23/2000	Sun Microsystems Inc.			
	C9	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp			
	C10	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp			
	C11	JP10-070531	03/10/1998	Brother Ind Ltd.			
	C12	JP62-214744	9/21/1987	Hitachi Ltd.			
	C13	WO0070458	11/23/2000	Comsec Corporation			
	C14	WO0017775	3/30/00	Miller et al.			
	C15	WO01016766	03/08/2001	Science Applications International Corporation			
	C16	WO0150688	7/12/01	Kriens			
	C17	WO9827783	06/25/1998	Northern Telecom Limited			
	C18	WO9855930	12/10/98	Tang			

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	C19	WO9843396	10/01/1998	Northern Telecom Limited			
	C20	WO9859470	12/30/98	Kanter et al.			
	C21	WO9911019	03/04/1999	V One Corp			
	C22	WO9938081	7/29/99	Paulsen et al.			
	C23	WO9948303	9/23/99	Cox et al.			
	C24	WO01/61922	02/12/2001	Science Application International Corporation			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D2	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D3	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D4	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D5	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	D6	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D7	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D8	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D9	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D10	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	D11	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	D12	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D13	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D14	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	D15	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D16	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D17	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	D18	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	D19	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	D20	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D21	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D22	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D23	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D24	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D25	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	D26	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D27	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conference on Communications architectures & protocols. pp. 84-91, ACM Press, NY, NY 1986.	
	D28	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D29	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	D30	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation.	
	D31	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D32	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D33	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) RFC1101, DNS SRV)	
	D34	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	D35	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	D37	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	D38	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	D39	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	D40	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	D41	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	D42	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	D43	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	
	D44	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	D45	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	D46	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	D47	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista)	
	D48	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	D49	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	D50	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)	
	D51	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/199706200300312/www.aventail.com/educate/whitepaper/ipmw.html (1997). (Corporate Access, Aventail)	
	D53	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	D54	Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschtag I, Onion Routing)	
	D55	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	D62	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	D63	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	D64	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	D65	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Definition, ANX)	
	D66	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	D67	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	
	D68	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	D69	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	D70	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	D71	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	D72	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	D73	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured there from and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	D74	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	D75	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (*available at* http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue). (NT Beta, Microsoft Prior Art VPN Technology)	
	D76	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D77	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	D78	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	D79	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	
	D80	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	D81	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). DISA, SIPRNET)	
	D82	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	D83	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	D84	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	D85	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	D86	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	D87	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	D88	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	
	D89	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	D90	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	D91	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	D92	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	D93	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	D94	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	D95	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	D96	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	D97	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	D98	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	D99	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*,<draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). Scott VPNs)	
	D101	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	D102	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	D103	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	D104	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	D105	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	D106	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	D107	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
	D108	Bhattacharya, et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	D109	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	D110	Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D111	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	D112	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	D113	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	D114	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	D115	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	D116	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	D117	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	D118	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	D119	Assured Digital Products. (Assured Digital)	
	D120	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	D121	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	D122	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	D123	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	D124	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	D125	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	
	D126	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	D127	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	D128	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	D129	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	D130	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	D131	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	D132	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	D140	Dan Sterne *et al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	
	D142	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	D143	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	D144	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	D145	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D147	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide - Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D148	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D149	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	D150	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	D154	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	D162	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/techneUarchive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	D165	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	D168	Kenneth Gregg, *et al., Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/enus/library/bb545687(VS.85.printer).aspx (Remote Access)	
	D170	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D171	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D172	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	D173	Microsoft Corp., Chapter 1 - Introduction to Windows NT Routing with Routing and Remote Access Service, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch0l.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	D174	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 - Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D175	F-Secure, *F-Secure NameSurfer*(May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) F-Secure VPN 3)	
	D177	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D185	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	D187	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	D189	F-Secure, *F-Secure VPN+ for Windows NT 4.0* (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., *SafeNet/Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., *About SafeNet / VPN Policy Manager* (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	D198	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	D204	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	D205	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	D206	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	D207	Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0* (September 21, 1998)	
	D209	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	D210	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	D211	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	D212	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	D213	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	D214	*Virtual Private Network Demonstration* (March 21, 1998)	
	D215	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	D216	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	D217	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	D218	Information Assurance, *Science Fair Agenda* (2000)	
	D219	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	D220	*IFE 3.1 Technology Dependencies* (2000)	
	D221	*IFE 3.1 Topology* (February 9, 2000)	
	D222	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	D224	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	13/339,257
	Filing Date	12-28-2011
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	77580-154(VRNK-1CP3CNFT4)

	D225	Information Assurance/NAI Labs, Dynamic Virtual Private Networks Presentation v.3 (2000)	
	D226	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	D228	Microsoft Corporation, *Microsoft Proxy Server 2.0* (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, *MCSE Test Success: Proxy Server 2*(1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D238	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	D239	*AutoSOCKS v2. 1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers, 1 99x/msg00945.html	
	D241	FirstVPN Enterprise Networks, Overview	
	D242	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	D243	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	D244	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	D245	Virtual Private Networks - Assured Digital Incorporated - ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	D246	Accessware - The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	D247	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	D248	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	D249	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	D250	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	
	D251	Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	D252	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	D253	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	D254	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	
	D255	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	D256	Davies and Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
	D257	Davies et al., "An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer," Security for Computer Networks, Second Edition, pp. 98-101 (1989)	
	D258	Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998)	
	D259	Chapman et al., "Domain Name System (DNS)," 278-296 (1995)	
	D260	Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D261	De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999)	
	D262	Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	
	D263	Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	
	D264	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D265	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D266	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87(1997)	
	D267	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	
	D268	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	D269	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D270	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D271	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D272	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D273	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	D274	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D275	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D276	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D277	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D278	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D279	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D280	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	
	D281	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	D282	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	D283	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	D284	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	D292	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages .	
	D293	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages .	
	D294	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages .	
	D295	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D296	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D297	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D298	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D299	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM	
	D300	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM	
	D301	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM	
	D302	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM	
	D303	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM	
	D304	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM	
	D305	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM	
	D306	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM	
	D307	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM	
	D308	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D309	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D310	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D311	Tannenbaum, "Computer Networks," pages 202-219 (1996)	
	D312	Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D315	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '211 Patent[2]	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '504 Patent[2]	
	D317	Exhibit 3, RFC 2543[1] vs. Claims of the '135 Patent[2]	
	D318	Exhibit 4, RFC 2543[1] vs. Claims of the '211 Patent[2]	
	D319	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent[2]	
	D320	Exhibit 6, SIP Draft v.2[1] vs. Claims of the '135 Patent[2]	
	D321	Exhibit 7, SIP Draft v.2[1] vs. Claims of the '211 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/339,257
	Filing Date	12-28-2011
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	77580-154(VRNK-1CP3CNFT4)

	D322	Exhibit 8, SIP Draft v.2[1] vs. Claims of the '504 Patent[2]	
	D323	Exhibit 9, H.323[1] vs. Claims of the '135 Patent[2]	
	D324	Exhibit 10, H.323[1] vs. Claims of the '211 Patent[2]	
	D325	Exhibit 11, H.323[1] vs. Claims of the '504 Patent[2]	
	D326	Exhibit 12, SSL 3.0[1] vs. Claims of the '135 Patent[2] .	
	D327	Exhibit 13, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D328	Exhibit 14, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D329	Exhibit 15, RFC 2487[1] vs. Claims of the '135 Patent[2]	
	D330	Exhibit 16, RFC 2487[1] vs. Claims of the '211 Patent[2]	
	D331	Exhibit 17, RFC 2487[1] vs. Claims of the '504 Patent[2]	
	D332	Exhibit 18, RFC 2595[1] vs. Claims of the '135 Patent[2]	
	D333	Exhibit 19, RFC 2595[1] vs. Claims of the '211 Patent[2]	
	D334	Exhibit 20, RFC 2595[1] vs. Claims of the '504 Patent[2]	
	D335	Exhibit 21, iPass[1] vs. Claims of the '135 Patent[2]	
	D336	Exhibit 22, iPASS[1] vs. Claims of the '211 Patent[2]	
	D337	Exhibit 23, iPASS[1] vs. Claims of the '504 Patent[2]	
	D338	Exhibit 24, "US '034"[1] vs. Claims of the '135 Patent[2]	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034")[1] vs. Claims of the '211 Patent[2]	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034")[1] vs. Claims of the '504 Patent[2]	
	D341	Exhibit 27, US '287[1] vs. Claims of the '135 Patent[2]	
	D342	Exhibit 28, US '287[1] vs. Claims of the '211 Patent[2]	
	D343	Exhibit 29, US '287[1] vs. Claims of the '504 Patent[2]	
	D344	Exhibit 30, Overview of Access VPNs[1] vs. Claims of the '135 Patent[2]	
	D345	Exhibit 31, Overview of Access VPNs[1] vs. Claims of the '211 Patent[2]	
	D346	Exhibit 32, Overview of Access VPNs[1] vs. Claims of the '504 Patent[2]	
	D347	Exhibit 34, RFC 1928[1] vs. Claims of the '135 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D348	Exhibit 35, RFC 1928[1] vs. Claims of the '211 Patent[2]	
	D349	Exhibit 36, RFC 1928[1] vs. Claims of the '504 Patent[2]	
	D350	Exhibit 37, RFC 2661[1] vs. Claims of the '135 Patent[2]	
	D351	Exhibit 38, RFC 2661[1] vs. Claims of the '211 Patent[2]	
	D352	Exhibit 39, RFC 2661[1] vs. Claims of the '504 Patent[2]	
	D353	Exhibit 40, SecureConnect[1] vs. Claims of the '135 Patent[2]	
	D354	Exhibit 41, SecureConnect[1] vs. Claims of the '211 Patent[2]	
	D355	Exhibit 42,SecureConnect[1] vs. Claims of the '504 Patent[2]	
	D356	Exhibit 43, SFS-HTTP[1] vs. Claims of the '135 Patent[2]	
	D357	Exhibit 44, SFS-HTTP[1] vs. Claims of the '211 Patent[2]	
	D358	Exhibit 45, SFS-HTTP[1] vs. Claims of the '504 Patent[2]	
	D359	Exhibit 46, US '883[1] vs. Claims of the '135 Patent[2]	
	D360	Exhibit 47, US '883[1] vs. Claims of the '211 Patent[2]	
	D361	Exhibit 48, US '883[1] vs. Claims of the '504 Patent[2]	
	D362	Exhibit 49, US '132[1] vs. Claims of the '135 Patent[2]	
	D363	Exhibit 50, US '132[1] vs. Claims of the '211 Patent[2]	
	D364	Exhibit 51, US '132[1] vs. Claims of the '504 Patent[2]	
	D365	Exhibit 52, US '213[1] vs. Claims of the '135 Patent[2]	
	D366	Exhibit 53, US '213[1] vs. Claims of the '211 Patent[2]	
	D367	Exhibit 54, US '213[1] vs. Claims of the '504 Patent[2]	
	D368	Exhibit 55, B&M VPNs[1] vs. Claims of the '135 Patent[2]	
	D369	Exhibit 56, B&M VPNs[1] vs. Claims of the '211 Patent[2]	
	D370	Exhibit 57, B&M VPNs[1] vs. Claims of the '504 Patent[2]	
	D371	Exhibit 58, BorderManager[1] vs. Claims of the '135 Patent[2]	
	D372	Exhibit 59, BorderManager[1] vs. Claims of the '211 Patent[2]	
	D373	Exhibit 60, BorderManager[1] vs. Claims of the '504 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D374	Exhibit 61, Prestige 128 Plus[1] vs. Claims of the '135 Patent[2]	
	D375	Exhibit 62, Prestige 128 Plus[1] vs. Claims of the '211 Patent[2]	
	D376	Exhibit 63, Prestige 128 Plus[1] vs. Claims of the '504 Patent[2]	
	D377	Exhibit 64, RFC 2401[1] vs. Claims of the '135 Patent[2]	
	D378	Exhibit 65, RFC 2401[1] vs. Claims of the '211 Patent[2]	
	D379	Exhibit 66, RFC 2401[1] vs. Claims of the '504 Patent[2]	
	D380	Exhibit 67, RFC 2486[1] vs. Claims of the '135 Patent[2]	
	D381	Exhibit 68, RFC 2486[1] vs. Claims of the '211 Patent[2]	
	D382	Exhibit 69, RFC 2486[1] vs. Claims of the '504 Patent[2]	
	D383	Exhibit 70, Understanding IPSec[1] vs. Claims of the '135 Patent[2]	
	D384	Exhibit 71, Understanding IPSec[1] vs. Claims of the '211 Patent[2]	
	D385	Exhibit 72, Understanding IPSec[1] vs. Claims of the '504 Patent[2]	
	D386	Exhibit 73, US '820[1] vs. Claims of the '135 Patent[2]	
	D387	Exhibit 74, US '820[1] vs. Claims of the '211 Patent[2]	
	D388	Exhibit 75, US '820[1] vs. Claims of the '504 Patent[2]	
	D389	Exhibit 76, US '019[1] vs. Claims of the '211 Patent[2]	
	D390	Exhibit 77, US '019[1] vs. Claims of the '504 Patent[2]	
	D391	Exhibit 78, US '049[1] vs. Claims of the '135 Patent[2]	
	D392	Exhibit 79, US '049[1] vs. Claims of the '211 Patent[2]	
	D393	Exhibit 80, US '049[1] vs. Claims of the '504 Patent[2]	
	D394	Exhibit 81, US '748[1] vs. Claims of the '135 Patent[2]	
	D395	Exhibit 82, US '261[1] vs. Claims of the '135 Patent[2]	
	D396	Exhibit 83, US '261[1] vs. Claims of the '211 Patent[2]	
	D397	Exhibit 84, US '261[1] vs. Claims of the '504 Patent[2]	
	D398	Exhibit 85, US '900[1] vs. Claims of the '135 Patent[2]	
	D399	Exhibit 86, US '900[1] vs. Claims of the '211 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	13/339,257
	Filing Date	12-28-2011
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	77580-154(VRNK-1CP3CNFT4)

	D400	Exhibit 87, US '900[1] vs. Claims of the '504 Patent[2]	
	D401	Exhibit 88, US '671[1] vs. Claims of the '135 Patent[2]	
	D402	Exhibit 89, US '671[1] vs. Claims of the '211 Patent[2]	
	D403	Exhibit 90, US '671[1] vs. Claims of the '504 Patent[2]	
	D404	Exhibit 91, JP '704[1] vs. Claims of the '135 Patent[2]	
	D405	Exhibit 92, JP '704[1] vs. Claims of the '211 Patent[2]	
	D406	Exhibit 93, JP '704[1] vs. Claims of the '504 Patent[2]	
	D407	Exhibit 94, GB '841[1] vs. Claims of the '135 Patent[2]	
	D408	Exhibit 95, GB '841[1] vs. Claims of the '211 Patent[2]	
	D409	Exhibit 96, GB '841[1] vs. Claims of the '504 Patent[2]	
	D410	Exhibit 97, US '318[1] vs. Claims of the '135 Patent[2]	
	D411	Exhibit 98, US '318[1] vs. Claims of the '211 Patent[2]	
	D412	Exhibit 99, US '318[1] vs. Claims of the '504 Patent[2]	
	D413	Exhibit 100, VPN/VLAN[1] vs. Claims of the '135 Patent[2]	
	D414	Exhibit 101, Nikkei[1] vs. Claims of the '135 Patent[2]	
	D415	Exhibit 102, NIKKEI[1] vs. Claims of the '211 Patent[2]	
	D416	Exhibit 103, NIKKEI[1] vs. Claims of the '504 Patent[2]	
	D417	Exhibit 104, Special Anthology[1] vs. Claims of the '135 Patent[2]	
	D418	Exhibit 105, Omron[1] vs. Claims of the '135 Patent[2]	
	D419	Exhibit 106, Gauntlet System[1] vs. Claims of the '135 Patent[2]	
	D420	Exhibit 107, Gauntlet System[1] vs. Claims of the '151 Patent[2]	
	D421	Exhibit 108, Gauntlet System[1] vs. Claims of the '180 Patent[2]	
	D422	Exhibit 109, Gauntlet System[1] vs. Claims of the '211 Patent[2]	
	D423	Exhibit 110, Gauntlet System[1] vs. Claims of the '504 Patent[2]	
	D424	Exhibit 111, Gauntlet System[1] vs. Claims of the '759 Patent[2]	
	D425	Exhibit 112, IntraPort System[1] vs. Claims of the '135 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/339,257
	Filing Date	12-28-2011
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	77580-154(VRNK-1CP3CNFT4)

	D426	Exhibit 113, IntraPort System[1] vs. Claims of the '151 Patent[2]	
	D427	Exhibit 114, IntraPort System[1] vs. Claims of the '180 Patent[2]	
	D428	Exhibit 115, IntraPort System[1] vs. Claims of the '211 Patent[2]	
	D429	Exhibit 116, IntraPort System[1] vs. Claims of the '504 Patent[2]	
	D430	Exhibit 117, IntraPort System[1] vs. Claims of the '759 Patent[2]	
	D431	Exhibit 118, Altiga VPN System[1] vs. Claims of the '135 Patent[2]	
	D432	Exhibit 119, Altiga VPN System[1] vs. Claims of the '151 Patent[2]	
	D433	Exhibit 120, Altiga VPN System[1] vs. Claims of the '180 Patent[2]	
	D434	Exhibit 121, Altiga VPN System[1] vs. Claims of the '211 Patent[2]	
	D435	Exhibit 122, Altiga VPN System[1] vs. Claims of the '504 Patent[2]	
	D436	Exhibit 123, Altiga VPN System[1] vs. Claims of the '759 Patent[2]	
	D437	Exhibit 124, Kiuchi[1] vs. Claims of the '135 Patent[2]	
	D438	Exhibit 125, Kiuchi[1] vs. Claims of the '151 Patent[2]	
	D439	Exhibit 126, Kiuchi[1] vs. Claims of the '180 Patent[2]	
	D440	Exhibit 127, Kiuchi[1] vs. Claims of the '211 Patent[2]	
	D441	Exhibit 128, Kiuchi[1] vs. Claims of the '504 Patent[2]	
	D442	Exhibit 129, Kiuchi[1] vs. Claims of the '759 Patent[2]	
	D443	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '135 Patent[2]	
	D444	Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '151 Patent[2]	
	D445	Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '180 Patent[2]	
	D446	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '211 Patent[2]	
	D447	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '504 Patent[2]	
	D448	Exhibit 135, Overview[1] vs. Claims of the '759 Patent[2]	
	D449	Exhibit 136, RFC 2401[1] vs. Claims of the '759 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D450	Exhibit 137, Schulzrinne[1] vs. Claims of the '135 Patent[2]	
	D451	Exhibit 138, Schulzrinne[1] vs. Claims of the '151 Patent[2]	
	D452	Exhibit 139, Schulzrinne[1] vs. Claims of the '180 Patent[2]	
	D453	Exhibit 140, Schulzrinne[1] vs. Claims of the '211 Patent[2]	
	D454	Exhibit 141, Schulzrinne[1] vs. Claims of the '504 Patent[2]	
	D455	Exhibit 142, Schulzrinne[1] vs. Claims of the '759 Patent[2]	
	D456	Exhibit 143, Solana[1] vs. Claims of the '135 Patent[2]	
	D457	Exhibit 144, Solana[1] vs. Claims of the '151 Patent[2]	
	D458	Exhibit 145, Solana[1] vs. Claims of the '180 Patent[2]	
	D459	Exhibit 146, Solana[1] vs. Claims of the '211 Patent[2]	
	D460	Exhibit 147, Solana[1] vs. Claims of the '504 Patent[2]	
	D461	Exhibit 148, Solana[1] vs. Claims of the '759 Patent[2]	
	D462	Exhibit 149, Atkinson[1] vs. Claims of the '135 Patent[2]	
	D463	Exhibit 150, Atkinson[1] vs. Claims of the '151 Patent[2]	
	D464	Exhibit 151, Atkinson[1] vs. Claims of the '180 Patent[2]	
	D465	Exhibit 152, Atkinson[1] vs. Claims of the '211 Patent[2]	
	D466	Exhibit 153, Atkinson[1] vs. Claims of the '504 Patent[2]	
	D467	Exhibit 154, Atkinson[1] vs. Claims of the '759 Patent[2]	
	D468	Exhibit 155, Marino[1] vs. Claims of the '135 Patent[2]	
	D469	Exhibit 156, Marino[1] vs. Claims of the '151 Patent[2]	
	D470	Exhibit 157, Marino[1] vs. Claims of the '180 Patent[2]	
	D471	Exhibit 158, Marino[1] vs. Claims of the '211 Patent[2]	
	D472	Exhibit 159, Marino[1] vs. Claims of the '504 Patent[2]	
	D473	Exhibit 160, Marino[1] vs. Claims of the '759 Patent[2]	
	D474	Exhibit 161, Aziz ('646)[1] vs. Claims of the '759 Patent[2]	
	D475	Exhibit 162, Wesinger[1] vs. Claims of the '135 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D476	Exhibit 163, Wesinger[1] vs. Claims of the '151 Patent[2]	
	D477	Exhibit 164, Wesinger[1] vs. Claims of the '180 Patent[2]	
	D478	Exhibit 165, Wesinger[1] vs. Claims of the '211 Patent[2]	
	D479	Exhibit 166, Wesinger[1] vs. Claims of the '504 Patent[2]	
	D480	Exhibit 167, Wesinger[1] vs. Claims of the '759 Patent[2]	
	D481	Exhibit 168, Aziz ('234)[1] vs. Claims of the '135 Patent[2]	
	D482	Exhibit 169, Aziz ('234)[1] vs. Claims of the '151 Patent[2]	
	D483	Exhibit 170, Aziz ('234)[1] vs. Claims of the '180 Patent[2]	
	D484	Exhibit 171, Aziz ('234)[1] vs. Claims of the '211 Patent[2]	
	D485	Exhibit 172, Aziz ('234)[1] vs. Claims of the '504 Patent[2]	
	D486	Exhibit 173, Aziz ('234)[1] vs. Claims of the '759 Patent[2]	
	D487	Exhibit 174, Schneider[1] vs. Claims of the '759 Patent[2]	
	D488	Exhibit 175, Valencia[1] vs. Claims of the '135 Patent[2]	
	D489	Exhibit 176, Valencia[1] vs. Claims of the '151 Patent[2]	
	D490	Exhibit 177, Valencia[1] vs. Claims of the '180 Patent[2]	
	D491	Exhibit 178, Valencia[1] vs. Claims of the '211 Patent[2]	
	D492	Exhibit 179, Valencia[1] vs. Claims of the '504 Patent[2]	
	D493	Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867[1] vs. Claims of the '180 Patent[2]	
	D494	Exhibit 181, Davison[1] vs. Claims of the '135 Patent[2]	
	D495	Exhibit 182, Davison[1] vs. Claims of the '151 Patent[2]	
	D496	Exhibit 183, Davison[1] vs. Claims of the '180 Patent[2]	
	D497	Exhibit 184, Davison[1] vs. Claims of the '211 Patent[2]	
	D498	Exhibit 185, Davison[1] vs. Claims of the '504 Patent[2]	
	D499	Exhibit 186, Davison[1] vs. Claims of the '759 Patent[2]	
	D500	Exhibit 187, AutoSOCKS v2.1[1] vs. Claims of the '135 Patent[2]	
	D501	Exhibit 188, AutoSOCKS v2.1[1] vs. Claims of the '151 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D502	Exhibit 189, AutoSOCKS v2.1 Administrator's Guide[1] vs. Claims of the '180 Patent[2]	
	D503	Exhibit 190, AutoSOCKS[1] vs. Claims of the '759 Patent[2]	
	D504	Exhibit 191, Aventail Connect 3.01/2.51[1] vs. Claims of the '135 Patent[2]	
	D505	Exhibit 192, Aventail Connect v3.01/2.51[1] vs. Claims of the '151 Patent[2]	
	D506	Exhibit 193, Aventail Connect 3.01/2.51[1] vs. Claims of the '180 Patent[2]	
	D507	Exhibit 194, Aventail Connect 3.01/2.51[1] vs. Claims of the '759 Patent[2]	
	D508	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the '135 Patent[2]	
	D509	Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the '151 Patent[2]	
	D510	Exhibit 197, Aventail Connect 3.1/2.6[1] vs. Claims of the '180 Patent[2]	
	D511	Exhibit 198, Aventail Connect 3.1/2.6[1] vs. Claims of the '759 Patent[2]	
	D512	Exhibit 199, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the '151 Patent[2]	
	D513	Exhibit 200, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the '135 Patent[2]	
	D514	Exhibit 201, BinGO! vs. Claims of the '180 Patent[2]	
	D515	Exhibit 202, BinGO! vs. Claims of the '759 Patent[2]	
	D516	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0)[1] vs. Claims of the '135 Patent[2]	
	D517	Exhibit 204, Domain Name System (DNS) Security[1] vs. Claims of the '211 Patent[2]	
	D518	Exhibit 205, Domain Name System (DNS) Security[1] vs. Claims of the '504 Patent[2]	
	D519	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '211 Patent[2]	
	D520	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '504 Patent[2]	
	D521	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent[2]	
	D522	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent[2]	
	D523	Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '504 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D524	Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '211 Patent[2]	
	D525	Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the '135 Patent[2]	
	D526	Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '135 Patent[2]	
	D527	Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '151 Patent[2]	
	D528	Exhibit 215, U.S. Patent No. 6,643,701[1] vs. Claims of the '135 Patent[2]	
	D529	Exhibit 216, U.S. Patent No. 6,643,701[1] vs. Claims of the '151 Patent[2]	
	D530	Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401[1] vs. Claims of the '151 Patent[2]	
	D531	Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401[1] vs. Claims of the '135 Patent[2]	
	D532	Exhibit 219, U.S. Patent No. 6,496,867[1] vs. Claims of the '211 Patent[2]	
	D533	Exhibit 220, U.S. Patent No. 6,496,867[1] vs. Claims of the '504 Patent[2]	
	D534	Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the '151 Patent[2]	
	D535	Exhibit 222, U.S. Patent No. 6,557,037[1] vs. Claims of the '211 Patent[2]	
	D536	Exhibit 223, U.S. Patent No. 6,557,037[1] vs. Claims of the '504 Patent[2]	
	D537	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '135 Patent[2]	
	D538	Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '151 Patent[2]	
	D539	Exhibit Cisco-1, Cisco's Prior Art Systems[1] vs. Claims of the '135 Patent	
	D540	Exhibit Cisco-2, Cisco's Prior Art Systems[1] vs. Claims of the '151 Patent	
	D541	Exhibit Cisco-3, Cisco's Prior Art Systems[1] vs. Claims of the '180 Patent	
	D542	Exhibit Cisco-4, Cisco's Prior Art Systems[1] vs. Claims of the '211 Patent	
	D543	Exhibit Cisco-5, Cisco's Prior Art Systems[1] vs. Claims of the '504 Patent	
	D544	Exhibit Cisco-6, Cisco's Prior Art Systems[1] vs. Claims of the '759 Patent	
	D545	Exhibit Cisco-7, Cisco's Prior Art PIX System[1] vs. Claims of the '759 Patent	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D546	Exhibit A: Copy of U.S. Patent No. 6,502,135	
	D547	Exhibit A: Copy of U.S. Patent No. 7,490,151	
	D548	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D549	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D550	Exhibit B-1: File History of U.S. Patent 6,502,135	
	D551	Exhibit B-2: Reexamination Record No. 95/001,269	
	D552	Exhibit C1: Claim Chart – Aventail Connect v3.1 (Patent No. 6,502,135)	
	D553	Exhibit C2: Claim Chart Aventail Connect V3.01 (Patent No. 6,502,135)	
	D554	Exhibit C-1: Copy of U.S. Patent No. 7,010,604	
	D555	Exhibit C2: Claim Chart Aventail Autosocks (Patent No. 7,490,151)	
	D556	Exhibit C1: Claim Chart Aventail Connect v3.01 (Patent No. 7,490,151)	
	D557	Exhibit C-2: Provisional Application 60/106,261	
	D558	Exhibit C3: Claim Chart Aventail AutoSOCKS (Patent No. 6,502,135)	
	D559	Exhibit C3: Claim Chart BinGO (Patent No. 7,490,151)	
	D560	Exhibit C-3: Provisional Application 60/137,704	
	D561	Exhibit C4: Claim Chart Wang (Patent No. 6,502,135)	
	D562	Exhibit C4: Claim Chart Beser (Patent No. 7,490,151)	
	D563	Exhibit C5: Claim Chart Beser (Patent No. 6,502,135)	
	D564	Exhibit C5: Claim Chart Wang (Patent No. 7,490,151)	
	D565	Exhibit C6: Claim Chart BinGO (Patent No. 6,502,135)	
	D566	Exhibit D: Memorandum Opinion in *VirnetX v. Microsoft.*	
	D567	Exhibit D-1: Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP – The Development of a Secure, Closed HPPT-Based Network on the Internet," Published in the Proceedings of SNDSS 1996.	
	D568	Exhibit D-10: D.E. Denning and G.M. Sacco, "Time-stamps in Key Distribution Protocols," Communications of the ACM, Vol. 24, N.8, pp. 533-536. August 1981.	
	D569	Exhibit D-11: C.I. Dalton and J.F. Griffin, "Applying Military Grade Security to the Internet," Proceedings of the 8th Joint European Networking Conference (JENC 8), (May 12-15 1997).	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D570	Exhibit D-12: Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based protocols Secure against Dictionary Attacks," 1992 IEEE Symposium on Security and Privacy (1992).	
	D571	Exhibit D-2: Copy of U.S. Pat. No. 5,898,830	
	D572	Exhibit D-3: Eduardo Solana and Jürgen Harms, "Flexible Internet Secure Transactions Based on Collaborative Domains,", Security Protocols Workshop 1997, pp. 37-51.	
	D573	Exhibit D-4: Copy of U.S. Pat. No. 6,119,234	
	D574	Exhibit D-5: Jeff Sedayao, "'Mosaic Will Kill My Network!' – Studying Network Traffic Patterns of Mosaic Use," in Electron. Proc. 2nd World Wide Web Conf.'94: Mosaic and the Web, Chicago, IL, Oct. 1994.	
	D575	Exhibit D-6: M. Luby Juels and R. Ostrovsky, "Security of Blind Digital Signatures," Crypto '97, LNCS 1294, pages 150-164, Springer-Verlag, Berlin, 1997.	
	D576	Exhibit D-8: David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).	
	D577	Exhibit D-9: Copy of U.S. Pat. No. 7,764,231	
	D578	Exhibit E-1: Claim Charts Applying Kiuchi and Other References to Claims of the '135 Patent.	
	D579	Exhibit E1: Declaration of Chris Hopen (Patent No. 6,502,135)	
	D580	Exhibit E1: Declaration of Chris Hopen (Patent No. 7,490,151)	
	D581	Exhibit E-2: Claim Charts Applying Wesinger and Other References to Claims of the '135 Patent.	
	D582	Exhibit E2: Declaration of Michael Fratto (Patent No. 6,502,135)	
	D583	Exhibit E2: Declaration of Michael Fratto (Patent No. 7,490,151)	
	D584	Exhibit E-3: Claim Charts Applying Solana and Other References to Claims of the '135 Patent.	
	D585	Exhibit E3: Declaration of James Chester (Patent No. 6,502,135)	
	D586	Exhibit E3: Declaration of James Chester (Patent No. 7,490,151)	
	D587	Exhibit E-4: Claim Charts Applying Aziz and Other References to Claims of the '135 Patent.	
	D588	Exhibit X1: Aventail Connect Administrator's Guide v3.1/v2.6., PP 1-20 (1996-1999)	
	D589	Exhibit X10: Copy of U.S. Patent No. 4,885,778	
	D590	Exhibit X11: Copy of U.S. Patent No. 6,615,357	
	D591	Exhibit X2: Aventail Connect Administrator's Guide v3.01/v2.51., PP 1-116 (1996-1999)	
	D592	Exhibit X3: Aventail AutoSOCKS Administration & User's Guide v2.1., PP 1-70 (1996-1999)	
	D593	Exhibit X4: Reed et al., "Proxies for Anonymous Routine," 12th Annuary Computer Security Applications Conference, San Diego, CA, December -9-13, pp 1-10 (1996).	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D594	Exhibit X5: Wang, The Broadband Forum Technical Report, "TR-025 – Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL," Issue 1.0; pp. 1-24 , v1.0 (1999).	
	D595	Exhibit X6: Copy of U.S. Patent No. 6,496,867	
	D596	Exhibit X7: BinGO! User's Guide Incorporating by Reference BinGO! Extended Feature Reference.	
	D597	Exhibit X7: Kent et al., "Security Architecture for the Internet Protocol, " Network Working Group Request for Comments (RFC) 2401, pp 1-70 (1998).	
	D598	Exhibit X8: Copy of U.S. Patent No. 6,182,141	
	D599	Exhibit X9: BinGO! User's Guide v1.6 (1999).	
	D600	Exhibit Y1: Aventail Extranet Server 3.0 Administrator's Guide.	
	D601	Exhibit Y10: Hanks, S., et al., RFC1701, "Generic Routing Encapsulation (GRE)," 1994, Is Accessbile at http://www.ietf.org/rfc/rfc1701.txt.	
	D602	Exhibit Y10: Socolofsky, T. et al., RFC 1180, "A TCP/IP Tutorial," January 1991.	
	D603	Exhibit Y11: Simpson, W., editor, RFC 1661, "The Point-to-Point Protocol (PPP)," July 1994.	
	D604	Exhibit Y11: Simpson, W., RFC1994, "PPP Challenge Handshake Authentication Protocol (CHAP)," 1996, http://www.ietf.org/rdc/rfc1994.txt.	
	D605	Exhibit Y12: Meyer, G., RFC 1968, "The PPP Encryption Control Protocol (ECP)," June 1996.	
	D606	Exhibit Y12: Perkins, D., RFC1171, "The Point-To-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-To-Point Links," 1990, Is Accessible at http://www.ietf.org/rfc/rfc1171.txt.	
	D607	Exhibit Y13: Kummert, H., RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)," September, 1998.	
	D608	Exhibit Y14: Townsley, W.M., et al., RFC 2661, "Layer Two Tunneling Protocol 'L2TP'," August 1999.	
	D609	Exhibit Y15: Pall, G.S., RFC 2118, "Microsoft Point-To-Point Encryption (MPPE) Protocol," March 1997.	
	D610	Exhibit Y16: Gross, G., et al., RFC 2364, "PPP Over AAL5," July 1998.	
	D611	Exhibit Y17: Srisuresh, P., RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations," August 1999.	
	D612	Exhibit Y18: Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993.	
	D613	Exhibit Y2: Goldschlag et al., "Hiding Routing Information" (1996).	
	D614	Exhibit Y3: Copy of U.S. Patent No. 5,950,519	
	D615	Exhibit Y4: Ferguson, P. and Huston, G., "What Is a VPN", The Internet Protocol Journal, Vol 1., No. 1 (June 1998 ("Ferguson").	
	D616	Exhibit Y5: Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC1034").	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/339,257
	Filing Date	12-28-2011
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	77580-154(VRNK-1CP3CNFT4)

	D617	Exhibit Y6: Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC1035").	
	D618	Exhibit Y8: Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997.	
	D619	Exhibit Y8: Woodburn, R.A., et al., RFC1241, "A Scheme for an Internet Encapsulation Protocol: Version 1," 1991.	
	D620	Exhibit Y9: Leech, M., et al., RFC 1928, "Socks Protocol Version 5," March 1996.	
	D621	Exhibit Y9: Simpson, W., RFC1853, "IP in IP Tunneling," 1995, Is Accessible at http://ww.ietf.org/rfc/rfc1583.txt.	
	D622	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 6,502,135)	
	D623	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 7,490,151)	
	D624	Request for Inter Partes Reexamination (Patent No. 6,502,135)	
	D625	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 6,502,135)	
	D626	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 7,490,151)	
	D627	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D628	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D629	Transmittal Letter (Patent No. 6,502,135)	
	D630	Transmittal Letter (Patent No. 7,490,151)	
	D631	Joint Claim Construction and Prehearing Statement	
	D632	Exhibit A: Agreed Upon Terms; P.R. 4-3 Joint Claims Construction and Prehearing Statement	
	D633	Exhibit B: Disputed Claim Terms; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D634	Exhibit C; VirnetX's Proposed Construction of Claim Terms and Supporting Evidence	
	D635	Exhibit D; Defendants' Intrinsic and Extrinsic Support; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D636	File History of U.S. Patent 6,839,759	
	D637	Exhibit B-4; VirnetX, Inc. v. Microsoft Corp., Case No. 6:07-cv-80, Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759 (E.D. Tex. Dec. 18, 2009)	
	D638	Exhibit D-2; Kent et al., "Security Architecture for the Internet Protocol," Internet Engineering Task Force, Internet Draft, (Feb. 1998)	
	D639	Exhibit D-3; Aziz et al., U.S. Patent 5,548,646 to Aziz et al., "System for Signatureless Transmission and Reception of Data Packets Between Computer Networks," Filed Sept. 15, 1994 and issued Aug. 20, 1996	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D640	Exhibit D-4; Yinger; U.S. Patent 5,960,204 to Yinger et al., "System and Method for Installing Applications on a Computer on an as needed basis, Filed on October 28, 1996 and Issued September 28, 1999	
	D641	Exhibit D-8; Barlow; U.S. Patent 5,204,961 to Barlow, "Computer Network Operating with Multilevel Hierarchical Security with Selectable Common Trust Realms and Corresponding Security Protocols," Filed on June 25, 1990 and Issued April 20, 1993	
	D642	Exhibit D-12; RFC 1122, Braden, "Requirements for Internet Hosts – Communication Layers," RFC 1122 (Oct. 1989)	
	D643	Exhibit D-13; RFC 791; Information Sciences Institute, "Internet Protocol," DARPA Internet Program Specification RFC 791 (Sept. 1981)	
	D644	Exhibit D-14; Caronni et al., "SKIP – Securing the Internet," 5th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '96) (June 19-21, 1996)	
	D645	Exhibit D-15; Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP), " IPSEC Work Group Draft (July 26, 1997)	
	D646	Exhibit E-1; Claim Charts Applying Kiuchi as a Primary Reference to the '759 Patent.	
	D647	Exhibit E-2; Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D648	Exhibit E-3; Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D649	Exhibit E-4; Claim Charts Applying Kent in view of Caronni as a Primary Combination of References to the '759 Patent	
	D650	Exhibit D-5; Edwards et al., "High Security Web Servers and Gateways," Computer Networks and ISDN System 29, pages 927-938 (Sept. 1997)	
	D651	Exhibit D-10; Lee et al., "Hypertext Transfer Protocol – HTTP/1.0," RFC 1945 (May 1996)	
	D652	Exhibit E-3; Claim Charts Applying Blum to Claims of the '151 Patent	
	D653	Exhibit B-1, File History of U.S. Patent 7,490,151	
	D654	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D655	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D656	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D657	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	
	D658	VirnetX Inc., V. Mitel Networks Corp.; Defendants' Joint Invalidity Contentions	
	D659	Exhibit 37, RFC 2661[1] vs. Claims of the '135 Patent [2]	
	D660	Exhibit 38, RFC 2661[1] vs. Claims of the '211 Patent [2]	
	D661	Exhibit 39, RFC 2661[1] vs. Claims of the '504 Patent [2]	
	D662	Exhibit 40, SecureConnect[1] vs. Claims of the '135 Patent [2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D663	Exhibit 41, SecureConnect[1] vs. Claims of the '211 Patent [2]	
	D664	Exhibit 42, SecureConnect[1] vs. Claims of the '504 Patent [2]	
	D665	Exhibit 43, SFS-HTTP[1] vs. Claims of the '135 Patent [2]	
	D666	Exhibit 44, SFS-HTTP[1] vs. Claims of the '211 Patent [2]	
	D667	Exhibit 45, SFS-HTTP[1] vs. Claims of the '504 Patent [2]	
	D668	Exhibit 46, US '883[1] vs. Claims of the '135 Patent [2]	
	D669	Exhibit 47, US '883[1] vs. Claims of the '211 Patent [2]	
	D670	Exhibit 48, US '883[1] vs. Claims of the '504 Patent [2]	
	D671	Exhibit 49, Chuah[1] vs. Claims of the '135 Patent [2]	
	D672	Exhibit 50, Chuah[1] vs. Claims of the '211 Patent [2]	
	D673	Exhibit 51, Chuah[1] vs. Claims of the '504 Patent [2]	
	D674	Exhibit 52, U.S. '648[1] vs. Claims of the '135 Patent [2]	
	D675	Exhibit 53, U.S. '648[1] vs. Claims of the '211 Patent [2]	
	D676	Exhibit 57, B&M VPNs[1] vs. Claims of the '504 Patent [2]	
	D677	Exhibit 58, BorderManager[1] vs. Claims of the '135 Patent [2]	
	D678	Exhibit 59, BorderManager[1] vs. Claims of the '211 Patent [2]	
	D679	Exhibit 60, BorderManager[1] vs. Claims of the '504 Patent [2]	
	D680	Exhibit 61, Prestige 128 Plus[1] vs. Claims of the '135 Patent [2]	
	D681	Exhibit 62, Prestige 128 Plus[1] vs. Claims of the '211 Patent [2]	
	D682	Exhibit 63, Prestige 128 Plus[1] vs. Claims of the '504 Patent [2]	
	D683	Exhibit 64, RFC 2401[1] vs. Claims of the '135 Patent [2]	
	D684	Exhibit 65, RFC 2401[1] vs. Claims of the '211 Patent [2]	
	D685	Exhibit 66, RFC 2401[1] vs. Claims of the '504 Patent [2]	
	D686	Exhibit 67, US '072[1] vs. Claims of the '135 Patent [2]	
	D687	Exhibit 68, RFC 2486[1] vs. Claims of the '211 Patent [2]	
	D688	Exhibit 69, RFC 2486[1] vs. Claims of the '504 Patent [2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D689	Exhibit 70 Understanding IPSec[1] vs. Claims of the '135 Patent [2]	
	D690	Exhibit 71, Understanding IPSec[1] vs. Claims of the '211 Patent [2]	
	D691	Exhibit 72, Understanding IPSec[1] vs. Claims of the '504 Patent [2]	
	D692	Exhibit 73, US '820[1] vs. Claims of the '135 Patent [2]	
	D693	Exhibit 74, US '820[1] vs. Claims of the '211 Patent [2]	
	D694	Exhibit 75, US '820[1] vs. Claims of the '504 Patent [2]	
	D695	Exhibit 76, US '019[1] vs. Claims of the '211 Patent [2]	
	D696	Exhibit 77, US '019[1] vs. Claims of the '504 Patent [2]	
	D697	Exhibit 78, US '049[1] vs. Claims of the '135 Patent [2]	
	D698	Exhibit 79, US '049[1] vs. Claims of the '211 Patent [2]	
	D699	Exhibit 80, US '049[1] vs. Claims of the '504 Patent [2]	
	D700	Exhibit 81, US '748[1] vs. Claims of the '135 Patent [2]	
	D701	Exhibit 82, US '261[1] vs. Claims of the '135 Patent [2]	
	D702	Exhibit 83, US '261[1] vs. Claims of the '211 Patent [2]	
	D703	Exhibit 84, US '261[1] vs. Claims of the '504 Patent [2]	
	D704	Exhibit 85, US '900[1] vs. Claims of the '135 Patent [2]	
	D705	Exhibit 86, US '900[1] vs. Claims of the '211 Patent [2]	
	D706	Exhibit 87, US '900[1] vs. Claims of the '504 Patent [2]	
	D707	Exhibit 88, US '671[1] vs. Claims of the '135 Patent [2]	
	D708	Exhibit 89, US '671[1] vs. Claims of the '211 Patent [2]	
	D709	Exhibit 90, US '671[1] vs. Claims of the '504 Patent [2]	
	D710	Exhibit 91, JP '704[1] vs. Claims of the '135 Patent [2]	
	D711	Exhibit 92, JP '704[1] vs. Claims of the '211 Patent [2]	
	D712	Exhibit 93, JP '704[1] vs. Claims of the '504 Patent [2]	
	D713	Exhibit 94, GB '841[1] vs. Claims of the '135 Patent [2]	
	D714	Exhibit 95, GB '841[1] vs. Claims of the '211 Patent [2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D715	Exhibit 96, GB '841[1] vs. Claims of the '504 Patent [2]	
	D716	Exhibit 97, US '318[1] vs. Claims of the '135 Patent [2]	
	D717	Exhibit 98, US '318[1] vs. Claims of the '211 Patent [2]	
	D718	Exhibit 99, US '318[1] vs. Claims of the '504 Patent [2]	
	D719	Exhibit 100, VPN/VLAN[1] vs. Claims of the '135 Patent [2]	
	D720	Exhibit 101, Nikkei[1] vs. Claims of the '135 Patent [2]	
	D721	Exhibit 102, Nikkei[1] vs. Claims of the '211 Patent [2]	
	D722	Exhibit 103, Nikkei[1] vs. Claims of the '504 Patent [2]	
	D723	Exhibit 104, Special Anthology[1] vs. Claims of the '135 Patent [2]	
	D724	Exhibit 106-A, Gauntlet System[1] vs. Claims of the '135 Patent [2]	
	D725	Exhibit 109-A, Gauntlet System[1] vs. Claims of the '211 Patent [2]	
	D726	Exhibit 110-A, Gauntlet System[1] vs. Claims of the '504 Patent [2]	
	D727	Exhibit 112, IntraPort System[1] vs. Claims of the '135 Patent [2]	
	D728	Exhibit 115, IntraPort System[1] vs. Claims of the '211 Patent [2]	
	D729	Exhibit 116, IntraPort System[1] vs. Claims of the '504 Patent [2]	
	D730	Exhibit 118, Altiga VPN System[1] vs. Claims of the '135 Patent [2]	
	D731	Exhibit 121, Altiga VPN System[1] vs. Claims of the '211 Patent [2]	
	D732	Exhibit 122, Altiga VPN System[1] vs. Claims of the '504 Patent [2]	
	D733	Exhibit 124, Kiuchi[1] vs. Claims of the '135 Patent [2]	
	D734	Exhibit 127, Kiuchi[1] vs. Claims of the '211 Patent [2]	
	D735	Exhibit 128, Kiuchi[1] vs. Claims of the '504 Patent [2]	
	D736	Exhibit 137, Schulzrinne[1] vs. Claims of the '135 Patent [2]	
	D737	Exhibit 137, Schulzrinne[1] vs. Claims of the '135 (Final) Patent [2]	
	D738	Exhibit 140, Schulzrinne[1] vs. Claims of the '211 Patent [2]	
	D739	Exhibit 141, Schulzrinne[1] vs. Claims of the '504 Patent [2]	
	D740	Exhibit 143, Solana[1] vs. Claims of the '135 Patent [2]	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D741	Exhibit 146, Solana[1] vs. Claims of the '211 Patent [2]	
	D742	Exhibit 147, Solana[1] vs. Claims of the '504 Patent [2]	
	D743	Exhibit 155, Marino[1] vs. Claims of the '135 Patent [2]	
	D744	Exhibit 158, Marino[1] vs. Claims of the '211 Patent [2]	
	D745	Exhibit 159, Marino[1] vs. Claims of the '504 Patent [2]	
	D746	Exhibit 168, Aziz[1] vs. Claims of the '135 Patent [2]	
	D747	Exhibit 171, U.S. '234[1] vs. Claims of the '211 Patent [2]	
	D748	Exhibit 172, Aziz[1] vs. Claims of the '504 Patent [2]	
	D749	Exhibit 175, Valencia[1] vs. Claims of the '135 Patent [2]	
	D750	Exhibit 178, Valencia[1] vs. Claims of the '211 Patent [2]	
	D751	Exhibit 179, Valencia[1] vs. Claims of the '504 Patent [2]	
	D752	Exhibit 181, Davison[1] vs. Claims of the '135 Patent [2]	
	D753	Exhibit 184, Davison[1] vs. Claims of the '211 Patent [2]	
	D754	Exhibit 185, Davison[1] vs. Claims of the '504 Patent [2]	
	D755	Exhibit 200, BinGO! User's Guide/Extended Features Reference[1] vs. Claims of the '135 Patent [2]	
	D756	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0)[1] vs. Claims of the '135 Patent [2]	
	D757	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '211 Patent [2]	
	D758	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '504 Patent [2]	
	D759	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent [2]	
	D760	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent [2]	
	D761	Exhibit 212, RFC 2486, RFC 2661, RFC 2401 and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the '135 Patent [2]	
	D762	Exhibit 218, U.S. Patent No. 6,496,867 in combination with RFC 2401"[1] vs. Claims of the '135 Patent [2]	
	D763	Exhibit 219, U.S. Patent No. 6,496,867[1] vs. Claims of the '211 Patent [2]	
	D764	Exhibit 220, U.S. Patent No. 6,496,867[1] vs. Claims of the '504 Patent [2]	
	D765	Exhibit 222, U.S. Patent No. 6,557,037[1] vs. Claims of the '211 Patent [2]	

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

/Krisna Lim/ 07/10/2012

13339257 - GAU: 2453

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D766	Exhibit 223, U.S. Patent No. 6,557,037[1] vs. Claims of the '504 Patent [2]	
	D767	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '135 Patent [2]	
	D768	Exhibit 228, U.S. 588[1] vs. Claims of the '211 Patent [2] (Final)	
	D769	Exhibit 229, U.S. 588[1] vs. Claims of the '504 Patent [2] (Final)	
	D770	Exhibit 230, Microsoft VPN[1] vs. Claims of the '135 Patent [2] (Final)	
	D771	Exhibit 231, Microsoft VPN[1] vs. Claims of the '211 Patent [2] (Final)	
	D772	Exhibit XX, Microsoft VPN[1] vs. Claims of the '504 Patent[2]	
	D773	Exhibit Cisco-1, Cisco's Prior Art System[1] vs. Claims of the '135 Patent[2]	
	D774	Exhibit Cisco-4, Cisco's Prior Art System[1] vs. Claims of the '211 Patent[2]	
	D775	Exhibit Cisco-5, Cisco's Prior Art System[1] vs. Claims of the '504 Patent[2]	
	D776	Exhibit 225, US '037[1] vs. Claims of the '135 Patent[2]	
	D777	Exhibit 226, ITU-T Standardization Activities[1] vs. Claims of the '135 Patent[2]	
	D778	Exhibit 227, US '393[1] vs. Claims of the '135 Patent[2]	
	D779	Exhibit 233, The Miller Application[1] vs. Claim 13 of the '135 Patent[2]	
	D780	Exhibit 234, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect")[1] vs. Claims of the '504 Patent[2]	
	D781	Exhibit 235, Microsoft VPN[1] vs. Claims of the '504 Patent[2]	
	D782	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; published January 1997[1] vs. Claims of the '211 Patent[2]	
	D783	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; published January 1997[1] vs. Claims of the '504 Patent[2]	
	D784	Exhibit 3, RFC 2543[1] vs. Claims of the '135 Patent[2]	
	D785	Exhibit 4, RFC 2543[1] vs. Claims of the '211 Patent[2]	
	D786	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent[2]	
	D787	Exhibit 6, SIP Draft v.2[1] vs. Claims of the '135 Patent[2]	
	D788	Exhibit 7, SIP Draft v.2[1] vs. Claims of the '211 Patent[2]	
	D789	Exhibit 8, SIP Draft v.2[1] vs. Claims of the '504 Patent[2]	
	D790	Exhibit 9, H.323[1] vs. Claims of the '135 Patent[2]	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D791	Exhibit 10, H.323[1] vs. Claims of the '211 Patent[2]	
	D792	Exhibit 11, H.323[1] vs. Claims of the '504 Patent[2]	
	D793	Exhibit 12, SSL 3.0[1] vs. Claims of the '135 Patent[2]	
	D794	Exhibit 13, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D795	Exhibit 14, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D796	Exhibit 15, RFC 2487[1] vs. Claims of the '135 Patent[2]	
	D797	Exhibit 16, RFC 2487[1] vs. Claims of the '211 Patent[2]	
	D798	Exhibit 17, RFC 2487[1] vs. Claims of the '504 Patent[2]	
	D799	Exhibit 18, RFC 2595[1] vs. Claims of the '135 Patent[2]	
	D800	Exhibit 21, iPass[1] vs. Claims of the '135 Patent[2]	
	D801	Exhibit 22, iPass[1] vs. Claims of the '211 Patent[2]	
	D802	Exhibit 23, iPass[1] vs. Claims of the '504 Patent[2]	
	D803	Exhibit 24, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 135 Patent[1]	
	D804	Exhibit 25, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 211 Patent[1]	
	D805	Exhibit 26, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 504 Patent[1]	
	D806	Exhibit 27, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 135 Patent[1]	
	D807	Exhibit 28, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 211 Patent[1]	
	D808	Exhibit 29, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 504 Patent[1]	
	D809	Exhibit 35, RFC 1928[1] vs. Claims of the '211 Patent[2]	
	D810	Exhibit 36, RFC 1928[1] vs. Claims of the '504 Patent[2]	
	D811	Exhibit 106, Gaunlet System and Gaunlet References[1] vs. Claims of the '135 Patent[2]	
	D812	Exhibit 109, Gaunlet System and Gaunlet References[1] vs. Claims of the '211 Patent[2]	
	D813	Exhibit 110, Gaunlet System[1] vs. Claims of the '504 Patent[2]	
	D814	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '135 Patent[2]	
	D815	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '211 Patent[2]	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	D816	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '504 Patent[2]	
	D817	Exhibit 149, Atkinson[1] vs. Claims of the '135 Patent[2]	
	D818	Exhibit 152, Atkinson[1] vs. Claims of the '211 Patent[2]	
	D819	Exhibit 153, Atkinson[1] vs. Claims of the '504 Patent[2]	
	D820	Exhibit 162, Wesinger[1] vs. Claims of the '135 Patent[2]	
	D821	Exhibit 165, Wesinger[1] vs. Claims of the '211 Patent[2]	
	D822	Exhibit 166, Wesinger[1] vs. Claims of the '504 Patent[2]	
	D823	Exhibit 187, AutoSOCKS v2.1[1] vs. Claims of the '135 Patent[2]	
	D824	Exhibit 191, Aventail Connect 3.01/2.51 ("Aventail Connect")[1] vs. Claims of the '135 Patent[2]	
	D825	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect")[1] vs. Claims of the '135 Patent[2]	
	D826	Exhibit 204, Domain Name System (DNS) Security[1] vs. Claims of the '211 Patent[2]	
	D827	Exhibit 205, Domain Name System (DNS) Security[1] ("DNS Security") vs. Claims of the '504 Patent[2]	
	D828	Exhibit 210, Lendenmann[1] vs. Claims of the '211 Patent[2]	
	D829	Exhibit 211, Lendenmann[1] vs. Claims of the '504 Patent[2]	
	D830	Exhibit 213, U.S. Patent No. 7,100,195 in combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '135 Patent[2]	
	D831	Exhibit 215, Aziz[1] vs. Claims of the '135 Patent[2]	
	D832	Cisco '180, Efiling Acknowledgment	
	D833	Exhibit A, U.S. Patent 7,188,180	
	D834	Exhibit B1, File History of U.S. Patent 7,188,180	
	D835	Exhibit B2, File History of U.S. Patent Application No. 09/588,209	
	D836	Exhibit B3, File History of Reexamination Control No. 95/001,270, Reexamination of U.S. 7,188,180 requested by Microsoft Corp	
	D837	Exhibit D1, "Lendenmann": Rolf Lendenman, Understanding OSF DCE 1.1 For AIX and OS/2, IBM International Technical Support Organization (Oct. 1995).	
	D838	Exhibit D5, "Schneier": Bruce Schneier, Applied Cryptography (1996)	
	D839	Exhibit D6, RFC 793; Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Specification RFC 793 (Sept. 1981)	
	D840	Exhibit D7, "Schimpf"; Brian C. Schimpf, "Securing Web Access with DCE," Presented at Network and Distributed System Security (Feb. 10-11, 1997)	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D841	Exhibit D8, "Rosenberry"; Ward Rosenberry, David Kenney, and Gerry Fisher, Understanding DCE (1993)	
	D842	Exhibit D9, Masys; Daniel R. Masys & Dixie B. Baker, "Protecting Clinical Data on Web Client Computers: The PCASSO Approach," Proceedings of the AMIA '98 Annual Symposium, Orlando, Florida (Nov. 7-11, 1998)	
	D843	Exhibit E1, Claim Charts Applying Lendenmann as a Primary Reference to the '180 Patent.	
	D844	Exhibit E2, Claim Charts Applying Kiuchi as a Primary Reference to the '180 Patent	
	D845	Exhibit E3, Claim Charts Applying Solana as a Primary Reference to the '180 Patent	
	D846	Exhibit E4, Claim Charts Applying Schimpf and Rosenberry as a Primary Reference to the '180 Patent	
	D847	Request for Inter Partes Reexamination of Patent No. 7,188,180	
	D848	Modified PTO Form 1449	
	D849	Request for Inter Partes Reexamination Transmittal Form No. 7,188,180	
	D850	Exhibit A; U.S. Patent 7,921,211 with Terminal Disclaimer	
	D851	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,921,211)	
	D852	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D853	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D854	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser)	
	D855	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D856	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D857	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D858	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D859	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D860	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D861	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D862	Exhibit X1, Solana, E. et al. "Flexible Internet Secure Transactions Based on Collaborative Domains"	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

	D863	Exhibit X2, U.S. Patent 6,557,037	
	D864	Exhibit X4, Atkinson, R., IETF RFC 2230, "Key Exchange Delegation Record for the DNS" (November 1997)	
	D865	Exhibit X6, Kent, et al., IETF RFC 2401, "Security Architecture for the Internet Protocol" (November 1998) Is Accessible at: http://www.ietf.org/rfc/rfc2401.txt	
	D866	Exhibit X7, Eastlake, D. et al., IETF RFC 2065, "Domain Name System Security Extensions" (January 1997) Is Accessible at: http://www.ietf.org/rfc/rfc2065.txt	
	D867	Exhibit X9, Guttman, E. et al., IETF RFC 2504, "Users' Security Handbook" (February 1999) Is Accessible At: http://www.ietf.org/rfc/rfc2504.txt	
	D868	Exhibit Y3, Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989 ("RFC1123").	
	D869	Exhibit Y4, Atkinson, R., RFC 1825, "Security Architecture for the Internet Protocol (August 1995) Is Accessible At: http://www.ietf.org/rfc/rfc1825.txt	
	D870	Exhibit Y5, Housley, R. et al., RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (January 1999) Is accessible At: http://www.ietf.org/rfc/rfc2459.txt	
	D871	Exhibit A, U.S. Patent 7,418,504	
	D872	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,418,504)	
	D873	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D874	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in view of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D875	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D876	Exhibit C4, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D877	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed, and Beser	
	D878	Exhibit C6, Claim Chart – USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D879	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D880	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D881	Exhibit D1, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Applce, Inc, Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act. 6:2010cv00417 (E.D. Tex)	
	D882	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. against Apple Inc. Based on the 7,418,504	
	D883	Exhibit X5, Eastlake, D., et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)" (March 1999)	
	D884	Exhibit X6, Kent, S. IETF RFC 2401, "Security Architecture for the Internet Protocol, (November1998) http://www.ietf.org/rfc/rfc2401.txt	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D885	Exhibit X8, Postel, J. et al., IETF RFC 920, "Domain Requirements" (October 1984) Is Accessible at http://www.ietf.org/rfc/rfc920.txt	
	D886	Exhibit X10, Reed, M. et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996.	
	D887	Request for Inter Partes Reexamination Transmittal form	
	D888	Transmittal Letter	
	D889	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D890	Exhibit D-7, "Thomas": Brian Thomas, "Recipe for E-Commerce, IEEE Internet Computing, (Nov.-Dec. 1997)	
	D891	Exhibit D-9, "Kent II": Stephen Kent & Randall Atkinson, "IP Encapsulating Security Payload (ESP)," Internet Engineering Task Force, Internet Draft (Feb. 1998)	
	D892	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser (Came from Inval. Cisco dtd 11/18/11)	
	D893	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D894	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D895	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D896	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D897	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D898	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D899	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D900	211 Request for Inter Partes Reexamination	
	D901	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D902	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D903	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D904	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D905	Exhibit C6, USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D906	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D907	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D908	504 Request for Inter Partes Reexamination	
	D909	Defendants' Supplemental Joint Invalidity Contentions	
	D910	Exhibit 226, Securing Web Access with DCE[1] vs. Claims of the '135 Patent[2]	
	D911	Exhibit 227, Securing Web Access with DCE[1] vs. Claims of the '151 Patent[2]	
	D912	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '135 Patent[2]	
	D913	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '151 Patent[2]	
	D914	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '180 Patent[2]	
	D915	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '211 Patent[2]	
	D916	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '504 Patent[2]	
	D917	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '759 Patent[2]	
	D918	Exhibit 234, U.S. '648[1] vs. Claims of the '135 Patent	
	D919	Exhibit 235, U.S. '648[1] vs. Claims of the '211 Patent	
	D920	Exhibit 236, U.S. '648[1] vs. Claims of the '504 Patent[2]	
	D921	Exhibit 237, U.S. '648[1] vs. Claims of the '135 Patent[2]	
	D922	Exhibit 238, Gauntlet System [1] vs. Claims of the '211 Patent[2]	
	D923	Exhibit 239, Gauntlet System [1] vs. Claims of the '504 Patent[2]	
	D924	Exhibit 240, Gauntlet System [1] vs. Claims of the '135 Patent[2]	
	D925	Exhibit 241, U.S. '588 [1] vs. Claims of the '211 Patent[2]	
	D926	Exhibit 242, U.S. '588 [1] vs. Claims of the '504 Patent[2]	
	D927	Exhibit 243, Microsoft VPN [1] vs. Claims of the '135 Patent[2]	
	D928	Exhibit 244, Microsoft VPN [1] vs. Claims of the '211 Patent[2]	
	D929	Exhibit 245, Microsoft VPN [1] vs. Claims of the '504 Patent[2]	
	D930	Exhibit 246, ITU-T Standardization Activities [1] vs. Claims of the '135 Patent[2]	
	D931	Exhibit 247, U.S. '393 [1] vs. Claims of the '135 Patent[2]	
	D932	Exhibit 248, The Miller Application [1] vs. Claim 13 of the '135 Patent[2]	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D933	Exhibit 249, Gauntlet System [1] vs. Claims of the '151 Patent[2]	
	D934	Exhibit 250, ITU-T Standardization Activities [1] vs. Claims of the '151 Patent[2]	
	D935	Exhibit 251, U.S. Patent No. 5,940,393 [1] vs. Claims of the '151 Patent[2]	
	D936	Exhibit 252, Microsoft VPN [1] vs. Claims of the '151 Patent[2]	
	D937	Exhibit 253, U.S. Patent No.6,324,648 [1] vs. Claims of the '151 Patent[2]	
	D938	Exhibit 254, U.S. Patent No.6,857,072 [1] vs. Claims of the '151 Patent[2]	
	D939	Exhibit A, Aventail Press Release, May 2, 1997	
	D940	Exhibit B, InfoWorld, "Aventail Delivers Highly Secure, Flexible VPN Solution," InfoWorld, page 64D, (1997)	
	D941	Exhibit C, Aventail AutoSOCKS v2.1 Administrator's Guide	
	D942	Exhibit D, Aventail Press Release, October 12, 1998	
	D943	Exhibit G, Aventail Press Release, May 26, 1999	
	D944	Exhibit H, Aventail Press Release, August 9, 1999	
	D945	Exhibit J, "Aventail ExtraNet Center 3.1: Security with Solid Management, Network Computing, June 28, 1999	
	D946	Petition in Opposition to Patent Owner's Petition to Vacate Inter Partes ReExamination Determination on Certain Prior Art	
	D947	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D948	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under U.S.C. § 311	
	D949	Exhibit C1, Claim Chart Aventail Connect v3.1	
	D950	Exhibit C2, Claim Chart Aventail Connect v3.01	
	D951	Exhibit C3, Claim Chart Aventail AutoSOCKS	
	D952	Exhibit C4, Claim Chart Wang	
	D953	Exhibit C5, Claim Chart Beser	
	D954	Exhibit C6, Claim Chart BINGO	
	D955	Exhibit X6, U.S. Patent 6,496,867	
	D956	Exhibit X10, U.S. Patent 4,885,778	
	D957	Exhibit X11, U.S. Patent 6,615,357	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D958	Exhibit Y3, U.S. Patent 5,950,519	
	D959	Request for Inter Partes Reexamination Transmittal Form	
	D960	Transmittal Letter	
	D961	Exhibit D, v3.1 Administrator's Guide	
	D962	Exhibit E-1, Claim Charts Applying Kiuchi to Various Claims of the '135 Patent	
	D963	Exhibit E-2, Claim Charts Applying Wesinger to Various Claims of the '135 Patent	
	D964	Exhibit E-3, Claim Charts Applying Solana to Various Claims of the '135 Patent	
	D965	Exhibit E-4, Claim Charts Applying Aziz to Various Claims of the '135 Patent	
	D966	Request for Inter Partes Reexamination Transmittal Form	
	D967	Request for Inter Partes Reexamination	
	D968	Request for Inter Partes Reexamination Transmittal Form 1449/PTO	
	D969	Exhibit C1, Claim Chart Aventail Connect v3.01	
	D970	Exhibit C2, Claim Chart Aventail AutoSOCKS	
	D971	Exhibit C3, Claim Chart BINGO	
	D972	Exhibit C4, Claim Chart Beser	
	D973	Exhibit C5, Claim Chart Wang	
	D974	Transmittal Letter	
	D975	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D976	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D977	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D978	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D979	Exhibit E-3, Claim Charts Applying Blum to Claims of the '151 Patent	
	D980	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D981	Exhibit E-5, Claim Charts Applying Kiuchi and Edwards, and Kiuchi, Edwards, and Martin to Claims of the '151 Patent	
	D982	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D983	Exhibit A, U.S. Patent 6,839,759	
	D984	Exhibit C-1, U.S. Patent 6,502,135	
	D985	Exhibit E-1, Claim Charts Applying Kiuchi, as Primary Reference to the '759 Patent	
	D986	Exhibit E-2, Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D987	Exhibit E-3, Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D988	Exhibit E-4, Claim Charts Applying Kent in View of Caronni as a Primary Combination of References to the '759 Patent	
	D989	Request for Inter Partes Reexamination Transmittal Form	
	D990	Request for Inter Partes Reexamination	
	D991	Request for Inter Partes Reexamination Transmittal(form 1449/PTO)	
	D992	Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D993	Request for Inter Partes Reexamination	
	D994	Request for Inter Partes Reexamination Transmittal Form	
	D995	Request for Inter Partes Reexamination	
	D996	Request for Inter Partes Reexamination Transmittal Form	
	D997	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D998	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D999	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D1000	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D1001	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D1002	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D1003	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1004	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1005	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D1006	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*		Application Number	**13/339,257**
		Filing Date	**12-28-2011**
		First Named Inventor	**Victor Larson**
		Art Unit	**2453**
		Examiner Name	**Krisna Lim**
		Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1007	Exhibit B1, File History of U.S. Patent 7,418,504	
	D1008	Exhibit B2, File History of U.S. Patent Application No. 09/558,210	
	D1009	Exhibit D-10, Gaspoz et al., "VPN on DCE: From Reference Configuration to Implementation," Bringing Telecommunication Services to the People – IS&N '95, Third International Conference on Intelligence in Broadband Services and Networks, October 1995 Proceedings, Lecture Notes in Computer Science, Vol. 998 (Springer, 1995)	
	D1010	Exhibit D-11, Copy of U.S. Patent No. 6,269,099	
	D1011	Exhibit D-11, Copy of U.S. Patent No. 6,560,634	
	D1012	Exhibit D-13, Pallen, "The World Wide Web," British Medical Journal, Vol. 311 at 1554 (Dec. 1995)	
	D1013	Exhibit D-14, Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21:120-126 (Feb. 1978)	
	D1014	Exhibit D-15, Copy of U.S. Patent No. 4,952,930	
	D1015	Exhibit D-17, Pfaffenberger, Netscape Navigator 3.0: Surfing the Web and Exploring the Internet, Academic Press (1996)	
	D1016	Exhibit D-18, Gittler et al., "The DCE Security Service," Hewlett-Packard Journal, pages 41-48 (Dec. 1995)	
	D1017	Exhibit D-6, Copy of U.S. Patent No. 5,689,641	
	D1018	Exhibit D-9, Lawton, "New Top-Level Domains Promise Descriptive Names," Sunworld Online, 1996	
	D1019	Exhibit E-1, Copy of Catalog Listing by IBM for RS/6000 Redbooks Collection which includes a Link to the *Lendenmann* reference. The link to the *Lendenmann* reference was archived at archive.org on December 7, 1998 and retrieved by the Wayback Machine	
	D1020	Exhibit E-10, copy of an Archived Version of the Lawton reference archived at archive.org on February 19, 1999 and retrieved by the Wayback Machine	
	D1021	Exhibit E-11, Abstracts of the Proceedings of the Symposium on Network and Distributed System Security, 1996, Archived at archive.org on April 10, 1997, and retrieved by the Wayback Machine	
	D1022	Exhibit E-12, 1996 Symposium on Network and Distributed System Security, Website Archived by archive.org (Apr. 10, 1997), Retrieved by the Wayback Machine at http://web.archive.org/web/19970410114853/http://computer.org/cspress/catalog/proc9.htm.	
	D1023	Exhibit E-13, Copy of Search Results for ISBN 0-12-553153-2 (Pfaffenberger) from www.isbnsearch.org	
	D1024	Exhibit F-1, Claim Charts applying Lendenmann as a Primary Reference to the '504 Patent.	
	D1025	Exhibit F-2, Claim Charts applying Aziz as a Primary Reference to the '504 Patent	
	D1026	Exhibit F-3, Claim Charts applying Kiuchi and Pfaffenberger as Primary References to the '504 Patent	
	D1027	Exhibit E-2, First Page of U.S. Patent No. 5,913,217 published June 15, 1999 and citing a portion of the Lendenmann reference as a prior art reference	
	D1028	Exhibit E-3, Request for Comments 2026, "The Internet Standards Process – Revision 3," October 1996	

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

/Krisna Lim/ 07/10/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1029	Exhibit E-4, First Page of U.S. 5,463,735, published October 31, 1995 and citing RFC 793 as a prior art Reference	
	D1030	Exhibit E-5, Copy of catalog listing from Boston University Digital Common Website, listing the Martin reference with an issue date of February 21, 1998	
	D1031	Exhibit E-6, Copy of Technical Reports Archive Listing from Boston University Computer Science Department which includes a link to the Martin paper. The link to the Martin paper was archived at archive.org on January 22, 1998 and Retrieved by the Wayback Machine	
	D1032	Exhibit E-7, Boston University Computer Science Department Technical Reports Instructions, available at: http://www.cs.bu.edu/techreports/INSTRUCTIONS	
	D1033	Exhibit E-8, U. Möller, "Implementation eines Anonymisierungsverfahrens für WWW-Zugriffe," Diplomarbeit, Universität Hamburg (July 16, 1999), citing to Martin at page 77.	
	D1034	Exhibit E-9, First page of U.S. 5,737,423, published April 7, 1998 and citing Schneier as Prior Art Reference	
	D1035	Request for Inter Partes ReExamination; U.S. Patent 7,418,504	
	D1036	Request for Inter Partes ReExamination Transmittal Form; U.S. Patent 7,418,504	
	D1037	Request for Inter Partes Reexamination Transmittal (Form 1449/PTO) 7,418,504	
	D1038	Exhibit C1, Claim Chart – USP 7,921,211 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1039	Exhibit C2, Claim Chart – USP 7,921,211 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1040	Exhibit C3, Claim Chart – USP 7,921,211 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1041	Exhibit C4, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2230 and further in conjunction with RFC 920, Reed and Beser	
	D1042	Exhibit C5, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1043	Exhibit C6, Claim Chart – USP 7,921,211relative to Beser, Alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1044	Exhibit C7, Claim Chart – USP 7,921,211 relative to RFC 2230, alone and in conjunction with RFC 2401, Reed, and Beser	
	D1045	Exhibit C8, Claim Chart – USP 7,921,211 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1046	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1047	Exhibit C1, Claim Chart – USP 7,418,504 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1048	Exhibit C2, Claim Chart – USP 7,418,504 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1049	Exhibit C3, Claim Chart – USP 7,418,504 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1050	Exhibit C5, Claim Chart – USP 7,418,504 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1051	Exhibit C6, USP 7,418,504 relative to Beser, alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1052	Exhibit C7, Claim Chart – USP 7,418,504 relative to RFC 2230, alone and in conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1053	Exhibit C8, Claim Chart – USP 7,418,504 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1054	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1055	Exhibit 226, Securing Web Access with DCE[1] vs. Claims of the '135 Patent[2]	
	D1056	Exhibit 227, Securing Web Access with DCE[1] vs. Claims of the '151 Patent[2]	
	D1057	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '135 Patent[2]	
	D1058	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '151 Patent[2]	
	D1059	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '180 Patent[2]	
	D1060	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '211 Patent[2]	
	D1061	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '504 Patent[2]	
	D1062	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '759 Patent[2]	
	D1063	Exhibit 234, U.S. '648[1] vs. Claims of the '135 Patent[2]	
	D1064	Exhibit 235, U.S. '648[1] vs. Claims of the '211 Patent[2]	
	D1065	Exhibit 236, U.S. '648[1] vs. Claims of the '504 Patent[2]	
	D1066	Exhibit 237, U.S. '072[1] vs. Claims of the '135 Patent[2]	
	D1067	Exhibit 238, Gauntlet System [1] vs. Claims of the '211 Patent[2]	
	D1068	Exhibit 239, Gauntlet System[1] vs. Claims of the '504 Patent[2]	
	D1069	Exhibit 240, Gauntlet System [1] vs. Claims of the '135 Patent[2]	
	D1070	Exhibit 241, U.S. '588 [1] vs. Claims of the '211 Patent[2]	
	D1071	Exhibit 242, U.S. '588 [1] vs. Claims of the '504 Patent[2]	
	D1072	Exhibit 243, Microsoft VPN [1] vs. Claims of the '135 Patent[2]	
	D1073	Exhibit 244, Microsoft VPN [1] vs. Claims of the '211 Patent[2]	
	D1074	Exhibit 245, Microsoft VPN [1] vs. Claims of the '504 Patent[2]	
	D1075	Exhibit 246, ITU-T Standardization Activities[1] vs. Claims of the '135 Patent[2]	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1076	Exhibit 247, U.S. '393[1] vs. Claims of the '135 Patent[2]	
	D1077	Exhibit 248, The Miller Application[1] vs. Claim 13 of the '135 Patent[2]	
	D1078	Exhibit 249, Gauntlet System [1] vs. Claims of the '151 Patent[2]	
	D1079	Exhibit 250, ITU-T Standardization Activities [1] vs. Claims of the '151 Patent[2]	
	D1080	Exhibit 251, U.S. Patent No. 5,940,393 [1] vs. Claims of the '151 Patent[2]	
	D1081	Exhibit 252, Microsoft VPN [1] vs. Claims of the '151 Patent[2]	
	D1082	Exhibit 253, U.S. Patent No.6,324,648 [1] vs. Claims of the '151 Patent[2]	
	D1083	Exhibit 254, U.S. Patent No.6,857,072 [1] vs. Claims of the '151 Patent[2]	
	D1084	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1085	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1086	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1087	Exhibit B1, File History of U.S. Patent 7,921,211	
	D1088	Exhibit B2, File History of U.S. Patent Application No. 10/714,849	
	D1089	Exhibit B4, *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009)	
	D1090	Exhibit D15, U.S. Patent 4,952,930	
	D1091	Exhibit F1, Claim Charts Applying Lendenmann as a Primary Reference to the '211 Patent	
	D1092	Exhibit F2, Claim Charts Applying Aziz as a Primary Reference to the '211 Patent	
	D1093	Exhibit F3, Claim Charts Applying Kiuchi and Pfaffenberger as Primary References to the '211 Patent	
	D1094	Exhibit 2, Letter and attachment from Ramzi Khazen, Counsel for VirnetX, to Dmitriy Kheyfits, Counsel for Cisco Systems (June 23, 2011)	
	D1095	Exhibit P, Malkin, "Dial-In Virtual Private Networks Using Layer 3 Tunneling"	
	D1096	Exhibit Q, Ortiz, "Virtual Private Networks: Leveraging the Internet"	
	D1097	Exhibit R, Keromytix, "Creating Efficient Fail-Stop Cryptographic Protocols"	
	D1098	Transcript of Markman Hearing Dated January 5, 2012	
	D1099	Declaration of John P. J. Kelly, Ph.D	
	D1100	Defendants' Responsive Claim Construction Brief; Exhibits A–P and 1-7	

/Krisna Lim/ 07/10/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1101	Joint Claim Construction and Prehearing Statement Dated 11/08/11	
	D1102	Exhibit A: Agreed Upon Terms Dated 11/08/11	
	D1103	Exhibit B: Disputed Claim Terms Dated 11/08/11	
	D1104	Exhibit C: VirnetX's Proposed Construction of Claim Terms and Supporting Evidence Dated 11/08/11	
	D1105	Exhibit D: Defendant's Intrinsic and Extrinsic Support Dated 11/08/11	
	D1106	Declaration of Austin Curry in Support of VirnetX Inc.'s Opening Claim Construction Brief	
	D1107	Declaration of Mark T. Jones Opening Claims Construction Brief	
	D1108	VirnetX Opening Claim Construction Brief	
	D1109	VirnetX Reply Claim Construction Brief	
	D1110	European Search Report from corresponding EP Application Number 11005789 (Our Ref.: 077580-0142)	
	D1111	European Search Report from corresponding EP Application Number 11005792 (Our Ref.: 077580-0143)	

/Krisna Lim/ 07/10/2012

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

Best Available Copy 3-12-12 13339257 - GAU: 2453

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OPAP MAR 09 2012 PATENT & TRADEMARK OFFICE IAP5

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

CERTIFICATION STATEMENT

X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application 13/339,257 claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

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

] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Date: 3/8/12

03/13/2012 MBLANCO 00000037 501133 13339257

01 FC:1806 180.00 DA

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

BM_US 32311803-1.077580.0154

3-12-12 13339257 GAU: 2453

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OPAP MAR 09 2012 PATENT & TRADEMARK OFFICE

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

CERTIFICATION STATEMENT

X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was ›reviously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the ›reviously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in ı priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application 13/339,257 claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, iled March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, ssued December 31, 2002.

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

] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby H. Kusmer

Date: 3/8/12

03/13/2012 MBLANCO 00000037 501133 13339257

01 FC:1806 180.00 DA

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

·M_US 32311803-1.077580.0154

Best Available Copy 3-12-12 13339257 GAU: 2453

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OPAP MAR 09 2012 PATENT & TRADEMARK OFFICE IAP5

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

CERTIFICATION STATEMENT

X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application 13/339,257 claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

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

] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby H. Kusmer

Date: 3/8/12

03/13/2012 MBLANCO 00000037 501133 13339257

01 FC:1806 180.00 DA

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

BM_US 32311803-1.077580.0154

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1131	Peter Alexander Invalidity Report	
	D1132	Defendants' Second Supplemental Joint Invalidity Contentions	
	D1133	Exhibit 118A, Altiga VPN System[1] vs. Claims of the '135 Patent [2]	
	D1134	Exhibit 119A, Altiga VPN System[1] vs. Claims of the '151 Patent [2]	
	D1135	Exhibit 120A, Altiga VPN System[1] vs. Claims of the '180 Patent [2]	
	D1136	Exhibit 121A, Altiga VPN System[1] vs. Claims of the '211 Patent [2]	
	D1137	Exhibit 122A, Altiga VPN System[1] vs. Claims of the '504 Patent [2]	
	D1138	Exhibit 123A, Altiga VPN System[1] vs. Claims of the '759 Patent [2]	
	D1139	Exhibit 12A, SSL 3.0[1] vs. Claims of the '135 Patent[2]	
	D1140	Exhibit 13A, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D1141	Exhibit 14A, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D1142	Exhibit 228A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '135 Patent[2]	
	D1143	Exhibit 229A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '151 Patent[2]	
	D1144	Exhibit 230A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '180 Patent[2]	
	D1145	Exhibit 231A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '211 Patent[2]	
	D1146	Exhibit 232A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '504 Patent[2]	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1147	Exhibit 233A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '759 Patent[2]	
	D1148	Exhibit 255, Schulzrinne[1] vs. Claims of the '135 Patent[2]	
	D1149	Exhibit 256, Schulzrinne[1] vs. Claims of the '504 Patent[2]	
	D1150	Exhibit 257, Schulzrinne[1] vs. Claims of the '211 Patent[2]	
	D1151	Exhibit 258, Schulzrinne[1] vs. Claims of the '151 Patent[2]	
	D1152	Exhibit 259, Schulzrinne[1] vs. Claims of the '180 Patent[2]	
	D1153	Exhibit 260, Schulzrinne[1] vs. Claims of the '759 Patent[2]	
	D1154	Exhibit 261, SSL 3.0[1] vs. Claims of the '151 Patent[2]	
	D1155	Exhibit 262, SSL 3.0[1] vs. Claims of the '759 Patent[2]	
	D1156	Exhibit 263, Wang[1] vs. Claims of the '135 Patent[2]	
	D1157	Wang[1] vs. Claims of the '504 Patent[2]	
	D1158	Wang[1] vs. Claims of the '211 Patent[2]	
	D1159	Exhibit 1, Alexander CV.pdf	
	D1160	Exhibit 2, Materials Considered by Peter Alexander	
	D1161	Exhibit 3, Cross Reference Chart	
	D1162	Exhibit 4, RFC 2543[1] vs. Claims of the '135 Patent	
	D1163	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent	
	D1164	Exhibit 6, RFC 2543[1] vs. Claims of the '211 Patent	
	D1165	Exhibit 7, The Schulzrinne Presentation[1] vs. Claims of the '135 Patent	
	D1166	Exhibit 8, The Schulzrinne Presentation[1] vs. Claims of the '504 Patent	
	D1167	Exhibit 9, The Schulzrinne Presentation[1] vs. Claims of the '211 Patent	
	D1168	Exhibit 10, The Schulzrinne Presentation[1] vs. Claims of the '151 Patent	
	D1169	Exhibit 11, The Schulzrinne Presentation[1] vs. Claims of the '180 Patent	
	D1170	Exhibit 12, The Schulzrinne Presentation[1] vs. Claims of the '759 Patent	
	D1171	Exhibit 13, SSL 3.0[2] vs. Claims of the '135 Patent	
	D1172	Exhibit 14, SSL 3.0[2] vs. Claims of the '504 Patent	
	D1173	Exhibit 15, SSL 3.0[2] vs. Claims of the '211 Patent	
	D1174	Exhibit 16, SSL 3.0[2] vs. Claims of the '151 Patent	
	D1175	Exhibit 17, SSL 3.0[2] vs. Claims of the '759 Patent	
	D1176	Exhibit 18, Kiuchi[1] vs. Claims of the '135 Patent	
	D1177	Exhibit 19, Kiuchi[1] vs. Claims of the '504 Patent	
	D1178	Exhibit 20, Kiuchi[1] vs. Claims of the '211 Patent	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1179	Exhibit 21, Kiuchi[1] vs. Claims of the '151 Patent	
	D1180	Exhibit 22, Kiuchi[1] vs. Claims of the '180 Patent	
	D1181	Exhibit 23, Kiuchi[1] vs. Claims of the '759 Patent	
	D1182	Exhibit 24, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '135 Patent	
	D1183	Exhibit 25, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '504 Patent	
	D1184	Exhibit 26, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '211 Patent	
	D1185	Exhibit 27, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '151 Patent	
	D1186	Exhibit 28	
	D1187	Exhibit 29, The Altiga System[1] vs. Claims of the '135 Patent	
	D1188	Exhibit 30, The Altiga System[1] vs. Claims of the '504 Patent	
	D1189	Exhibit 31, The Altiga System[1] vs. Claims of the '211 Patent	
	D1190	Exhibit 32, The Altiga System[1] vs. Claims of the '759 Patent	
	D1191	Exhibit 33, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '135 Patent	
	D1192	Exhibit 34, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '504 Patent	
	D1193	Exhibit 35, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '211 Patent	
	D1194	Exhibit 36, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '151 Patent	
	D1195	Exhibit 37, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '180 Patent	
	D1196	Exhibit 38, Kent[1] vs. Claims of the '759 Patent	
	D1197	Exhibit 39, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent[2]	
	D1198	Exhibit 40, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent[2]	
	D1199	Exhibit 41, Aziz ('646)[1] vs. Claims of the '759 Patent	
	D1200	Exhibit 42, The PIX Firewall[1] vs. Claims of the '759 Patent	
	D1201	Exhibit A-1, Kiuchi[1] vs. Claims of the '135 Patent[2]	
	D1202	Exhibit B-1, Kiuchi[1] vs. Claims of the '211 Patent[2]	
	D1203	Exhibit C-1, Kiuchi[1] vs. Claims of the '504 Patent[2]	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1204	Exhibit D, Materials Considered	
	D1205	Exhibit E, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1206	Exhibit F, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1207	Exhibit G, Opening Expert Report of Dr. Stuart Stubblebine Regarding Invalidity of the '135, '211, and '504 Patents	

EXAMINER /Krisna Lim/	DATE CONSIDERED 07/10/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

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

Toby H Kusmer

Date: 6/1/12

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

DM_US 35535713-1.077580.0154

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-0001CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1119	Hopen Transcript dated April 11, 2012	
	A1120	VirnetX Claim Construction Opinion	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	07/10/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-0001CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

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

Toby H Kusmer

Date: May 3, 2012

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

DM_US 34026681-1.077580.0154

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

Best Available Copy 3-12-12 13339257 ~~GAU~~ 2453

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OPAP MAR 09 2012 IAP5 PATENT & TRADEMARK OFFICE

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

CERTIFICATION STATEMENT

X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application 13/339,257 claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

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

] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

[signature]

Date: 3/8/12

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

03/13/2012 MBLANCO 00000037 501133 13339257
01 FC:1806 180.00 DA

BM_US 32311803-1.077580.0154

Box 11 of 16.   3-12-12   13339257 GAU: 2453

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OPAP
MAR 09 2012
PATENT & TRADEMARK OFFICE

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

CERTIFICATION STATEMENT

X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application 13/339,257 claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

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

] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby H. Kusmer

Date: 3/8/12

03/13/2012 MBLANCO 00000037 501133 13339257

01 FC:1806 180.00 DA

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

M_US 32311803-1.077580.0154

Box 13 of 16.

3-12-12

13339257 GAU: 2453

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

OIPE IAP5 MAR 09 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application 13/339,257 claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

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

] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby H. Kusmer

Date: 3/8/12

03/13/2012 MBLANCO 00000037 501133 13339257

01 FC:1806 180.00 DA

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

BM_US 32311803-1.077580.0154

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number4-Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1215	Alexander Invalidity Expert Report dtd May 22, 2012 with Exhibits	
	D1216	Deposition of Peter Alexander dtd July 27, 2012	
	D1217	Cisco '151 Comments by Third Party Requester dtd August 17, 2012 with Exhibits	
	D1218	Cisco '151 Petition to Waive Page Limit Requirement for Third Party Comments dtd August 17, 2012	
	D1219	Deposition of Stuart Stubblebine dtd August 22, 2012	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Hasan M. Rashid

Date: 8/27/12

Hasan M. Rashid; Reg. No.:62,390
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 37791246-1.077580.0154

Electronic Acknowledgement Receipt

EFS ID:	13595759
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	27-AUG-2012
Filing Date:	28-DEC-2011
Time Stamp:	15:45:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	64501 d8e2b8595fe0890e455209592e2e1d932f5946ba	no	2

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Non Patent Literature	D1215part1_.pdf	6004542 ba8668057be3412bd85bc98b35f3ffbc3063d76a	no	1446
Warnings:					
Information:					
3	Non Patent Literature	D1215part2.pdf	3005505 cbda41f5d61322bb782a091b07a127acf9538b03	no	96
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Non Patent Literature	D1216.pdf	253751 2bedf1012dc0d5ca841e8957fd504aaa3c8d9a2e	no	55
Warnings:					
Information:					
5	Non Patent Literature	D1217.pdf	11161127 15c3902ff98d5442223a0deb429324c4c088740f	no	211
Warnings:					
Information:					
6	Non Patent Literature	D1218.pdf	171392 4de801f2c5f80805bb67088e6b5e9cc7c3df0153	no	4
Warnings:					
Information:					
7	Non Patent Literature	D1219.pdf	300469 88a75e44bb96dc311611481970f8b2ebfb3d2fee	no	69
Warnings:					
Information:					
			Total Files Size (in bytes):	20961287	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	12/28/2011	Victor Larson	77580-154(VRNK-1CP3CNFT4)	1084

23630 7590 08/31/2012
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
08/31/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Applicant-Initiated Interview Summary	Application No. 13/339,257	Applicant(s) LARSON ET AL.	
	Examiner KRISNA LIM	**Art Unit** 2453	

All participants (applicant, applicant's representative, PTO personnel):

(1) *KRISNA LIM*. (3)_____.

(2) *Toby Kusmer*. (4)_____.

Date of Interview: *08/23/2012*.

Type: ☐ Telephonic ☐ Video Conference
☒ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Wesinger (U.S. Patent No. 5,898,830)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Counsel and Examiner discussed the claimed language and the teaching of Wesinger; however no agreement is reached..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Krisna Lim/
Primary Examiner, Art Unit 2453

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1220	Defendants' Motion For Reconsideration of the Construction of the Term "Secure Communication Link," 7 pages, June 2012	
	D1221	Green, "Cisco Leverages Altiga Technology for VPN's," 2 pages, 2000 http://www.crn.com/news/channel-programs/18807923/cisco-leverages-altiga-technology-for-vpns.htm	
	D1222	Altiga Networks Archived at http://web.archive.org/web/20000823023437/http:/www.altiga.com/products/ 1999 and Retrieved by the Wayback Machine	
	D1223	Kiuchi, "C-HTTP The Development of a Secure, Closed HTTP-Based Network on the Internet," Department of Epidemiology and Biostatistics, Faculty of Medicine, University of Tokyo, Japan	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Date: 9/24/12

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

DM_US 38997101-1.077580.0154

Electronic Acknowledgement Receipt

EFS ID:	13821875
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	24-SEP-2012
Filing Date:	28-DEC-2011
Time Stamp:	16:12:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	69294 0700088ccc5b9a172c9be00e937852671fdb1e75	no	2

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

2	Non Patent Literature	D1220.pdf	123661 9ce2ace217ce1e1fbae718ae13ac16c56293 41a3	no	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:

3	Non Patent Literature	D1221.pdf	142693 2ebd0940ee6e4b3f4a822663b789030d32c 09246	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:

4	Non Patent Literature	D1222.pdf	69973 babcedd540231da1cc3e3494f36e2cbdfb1f f7d7	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:

5	Non Patent Literature	D1223.pdf	638867 00410f7202c99c99c2f118d5fbe6a3adb834 61be	no	42

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):	1044488

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1224	Lee et al., "Uniform Resource Locators (URL)," Network Working Group, RFC 1738, , December 1994 (25 pages)	
	D1225	VPN 3000 Concentrator Series, User Guide; Release 2.5 July 2000 (489 pages)	
	D1226	VPN 3000 Concentrator Series, Getting Started; Release 2.5 July 2000 (122 pages)	
	D1227	Fratto, Altiga Concentrates on VPN Security (Hardware Review Evaluation), Network Computing, March 22, 1999 (2 pages)	
	D1228	Response to RFP: Altiga, Network World Fusion, May 10, 1999 (7 pages)	
	D1229	Altiga Proves Multi-Vendor Interoperability for Seamless VPN Deployment; VPN Workshop Marks Significant Development in the VPN Market, July 12, 1999 (2 pages)	
	D1230	Altiga VPN Concentrator Series (C50) Versus Nortel Networks Contivity Extranet Switch 4000 and 4500, VPN Tunneling competitive Evaluation, 1999 (6 pages)	
	D1231	VPN 3000 Client User Guide, Release 2.5, July 2000 (94 pages)	
	D1232	Digital Certificates Design Specification for Release 2.0, May 17, 1999 (21 pages)	
	D1233	Altiga IPSec Client Architecture, Revision 1.0, April 5, 1999 (34 pages)	
	D1234	Altiga IPSec Functional Specification, Revision 2.1, (17 pages)	
	D1235	Altiga Product Requirements, Revision 1.7, May 26, 1998 (17 pages)	
	D1236	Altiga Network Lists Feature Functional Specification, Revision 1.0, (7 pages)	
	D1237	Altiga Split Tunneling Functional/Design Specification, (15 pages)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1238	Altiga Digital Certificate Support for IPSec Client V2.1 Functional Specification, August 12, 1999 (24 pages)	
	D1239	Altiga IPSec LAN to LAN Tunnel Autodiscovery Functional Specification, (5 pages)	
	D1240	Altiga Split Tunneling Testplan, Revision 1.0, (8 pages)	
	D1241	Altiga VPN Concentrator Getting Started, Revision 1, March 1999 (116 pages)	
	D1242	Altiga VPN Concentrator Getting Started, Version 2, June 1999 (102 pages)	
	D1243	Altiga VPN Concentrator Getting Started, Version 3, December 1999 (130 pages)	
	D1244	Altiga VPN Concentrator Getting Started, Version 4, March 2000 (138 pages)	
	D1245	Altiga VPN Concentrator User Guide, Revision 1, March 1999 (304 pages)	
	D1246	Altiga VPN Concentrator User Guide, Revision 1.1, March 1999 (304 pages)	
	D1247	Altiga VPN Concentrator User Guide, Version 3, June 1999 (478 pages)	
	D1248	Altiga VPN Concentrator User Guide, Version 4, December 1999 (472 pages)	
	D1249	Altiga VPN Concentrator User Guide, Version 5, March 2000 (606 pages)	
	D1250	Altiga VPN Client Installation and User Guide, Version 2, July 1999 (92 pages)	
	D1251	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 3, December 1999 (113 pages)	
	D1252	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 4, March 2000 (118 pages)	
	D1253	Altiga Networks VPN Concentrator and VPN Client, as well as their Public Demonstrations and Testing, are also Described in Marketing Materials and Publications (4 pages)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby H Kusmer

Date: 10/3/12

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

DM_US 39145292-1.077580.0154

Electronic Acknowledgement Receipt

EFS ID:	13917318
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	05-OCT-2012
Filing Date:	28-DEC-2011
Time Stamp:	11:48:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	96054 e39e4075ad301166fcaf8093635c6bd9e175866c	no	3

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Non Patent Literature	D1224.PDF	1385009 c0c023e1ffceb4909f65537ac685570ce89000f0	no	25
Warnings:					
Information:					
3	Non Patent Literature	D1225Part1.pdf	9707771 6ae528c44629d766c9fc4b776551d2680e925075	no	244
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Non Patent Literature	D1225Part2.pdf	8053147 7222d5e4fd698a15af27a75609a6ac57f6c9b5f7	no	245
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Non Patent Literature	D1226.PDF	9200782 8580c9a4640bf44fb6e2957b63f29a731ecfc9df	no	122
Warnings:					
Information:					
6	Non Patent Literature	D1227.PDF	1923180 c3f5782b90fe6dd48d635c349d737d268f6cff2e	no	2
Warnings:					
Information:					
7	Non Patent Literature	D1228.PDF	4527086 38650c0ad25030424906589531 82f34c882385d5	no	7
Warnings:					
Information:					
8	Non Patent Literature	D1229.PDF	1921619 8a30921b2a6d77e3745af10f4b4208a362fbdd58	no	2
Warnings:					
Information:					
9	Non Patent Literature	D1230.PDF	7300485 bc94176849e0031bdfa94581437d293ad31e622a	no	6

Warnings:					
Information:					
10	Non Patent Literature	D1231.PDF	6455029 1dae9c7575280f98a1b9665ebecf8047f644e308	no	94
Warnings:					
Information:					
11	Non Patent Literature	D1232.PDF	936879 a64c3cc70a981e525fa1c2a0856466016fec4742	no	21
Warnings:					
Information:					
12	Non Patent Literature	D1233.PDF	2643873 0ad9db0a2c4d60a911bbea292e560645569beb42	no	34
Warnings:					
Information:					
13	Non Patent Literature	D1234.PDF	1337280 26f30a98ca4b3c06dee097790ecccd22ed1cd625	no	17
Warnings:					
Information:					
14	Non Patent Literature	D1235.PDF	1118077 570378cf0fef9a9f0db5934767a10631a9697ccb	no	17
Warnings:					
Information:					
15	Non Patent Literature	D1236.PDF	516087 43622ea13fa2edcf841bf78b01ea08c61eccef68	no	7
Warnings:					
Information:					
16	Non Patent Literature	D1237.PDF	978889 cb31cc3954935b83adf852ae9cd68114d72e63d9	no	15
Warnings:					
Information:					
17	Non Patent Literature	D1238.PDF	2081715 7b840029a950da75a9c9adb76c6f30c69e188862	no	24
Warnings:					
Information:					
18	Non Patent Literature	D1239.PDF	329750 2d833f9187957eedcb0e407a1356ea87c36e052e	no	5

Warnings:					
Information:					
19	Non Patent Literature	D1240.PDF	507540 a74f5d5fbe671acf2414f22eaec9bbb487ffb0e2	no	8
Warnings:					
Information:					
20	Non Patent Literature	D1241.PDF	6401651 62ec4bfa8bce771c05b216d7c47c403a52973f36	no	116
Warnings:					
Information:					
21	Non Patent Literature	D1242.PDF	5607358 8f2f53edf2efb6f020153bbe73c2b562a03bb4f7	no	102
Warnings:					
Information:					
22	Non Patent Literature	D1243.PDF	7301095 3e89def78808ab4f8f5ce0b234cd3322f595cd61	no	130
Warnings:					
Information:					
23	Non Patent Literature	D1244.PDF	7945433 417911827dcb8d869eb9e217f1414dc9c4a46f9d	no	138
Warnings:					
Information:					
24	Non Patent Literature	D1245.PDF	17791506 735e0d644c3a58450a4b6cf096d32db096ca6d70	no	304
Warnings:					
Information:					
25	Non Patent Literature	D1246.PDF	17791522 be912d02c9cba1b615568dab376ef177ef963f86	no	304
Warnings:					
Information:					
26	Non Patent Literature	D1247part1.pdf	4478737 1b2222ad6d47bcf50238e51eae6b681ee70f4342	no	244
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

27	Non Patent Literature	D1247part2.pdf	4380602 f9d82845d47589474fcfc6f26b8fe686384cc ef5	no	234

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

28	Non Patent Literature	D1248part1.pdf	5121910 110aa00905f6405ddd299e00b45cf87c676 21cd0	no	239

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

29	Non Patent Literature	D1248part2.pdf	4580517 8369e89c947d049595d9e6451f6f84006b9 49fc4	no	233

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

30	Non Patent Literature	D1249part1.pdf	4350698 6ce20ea7a52e3038ca51c565713640627d2 30135	no	205

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

31	Non Patent Literature	D1249part2.pdf	4232123 2bdcf1c426a5631c6be840dc2307b3a0751 b50b2	no	198

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

32	Non Patent Literature	D1249part3.pdf	3557941 200eca2c1f3735e7560f74449c981de15557 3a10	no	203

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

33	Non Patent Literature	D1250.PDF	4663415 eedc19be973a322d4836e6d220271020c08 2e15f	no	92

Warnings:

Information:					
34	Non Patent Literature	D1251.PDF	5973935 fac713d79db8ae257186853a6ddb06f093b63bec	no	113
Warnings:					
Information:					
35	Non Patent Literature	D1252.PDF	6581540 2caebc0aacfb81210ecf5bbcf02440006b76a065	no	118
Warnings:					
Information:					
36	Non Patent Literature	D1253.PDF	1740859 7ea0a705b2f08195bb7ab0b072b732bef178620e	no	4
Warnings:					
Information:					
			Total Files Size (in bytes):	173521094	

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	12/28/2011	Victor Larson	77580-154(VRNK-1CP3CNFT4)	1084

23630 7590 10/18/2012

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

EXAMINER	
LIM, KRISNA	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
10/18/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

PTOL-90A (Rev. 04/07)

Applicant-Initiated Interview Summary	**Application No.** 13/339,257	**Applicant(s)** LARSON ET AL.	
	Examiner KRISNA LIM	**Art Unit** 2453	

All participants (applicant, applicant's representative, PTO personnel):

(1) *KRISNA LIM*.

(2) *Mr. Toby Kusmer (Reg. No. 26,418)*.

(3) *Mr. Robert Short*.

(4) ______.

Date of Interview: *11 October 2012*.

Type: ☐ Telephonic ☐ Video Conference
☒ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: ______.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Wesinger (Patent No. 5,898,830)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Mr. Short discussed the background and the gist of the invention. Mr. Short distinghished the gist feature of the invention in comparision to the firewall, the switch and the rounter of the prior arts. Mr. Short and Mr. Kusmer discussed the gist features of the invention. For example, the invention is focus on the feature of "intercepting domain name request look up and determining the request corresponding to the secure web site". .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Krisna Lim/
Primary Examiner, Art Unit 2453

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson *et al.*	:	
	:	
Serial No.: 13/339,257	:	Confirmation No. 1084
	:	
Filed: December 28, 2011	:	Group Art Unit: 2453
	:	
Customer Number: 23630		Examiner: Lim, Krisna

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

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

REPLY "B"

Sir:

This Reply is being filed in response to the Office Action mailed from the United States Patent and Trademark office on July 30, 2012.

Applicants appreciate the Examiner's thorough examination of the subject application and request reconsideration and further examination in view of the following:

Claims begin on page 2 of this paper.

Remarks begin on page 6 of this paper.

IN THE CLAIMS

The claims are being presented solely for the convenience of the Office. No claims are being added, amended, deleted, or canceled.

LISTING OF CLAIMS:

1. (Original) A method of connecting a first network device and a second network device, the method comprising:

    receiving, from the first network device, a request to look up a network address of the second network device based on an identifier associated with the second network device;

    determining, in response to the request, whether the second network device is available for a secure communications service; and

    initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

    wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

2. (Original) The method of claim 1, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

3. (Original) The method of claim 1, wherein the secure communication link is a virtual private network communication link.

4. (Original) The method of claim 1, wherein the secure communications service includes a video conferencing service.

5. (Original) The method of claim 1, wherein the secure communications service includes a telephony service.

6. (Original) The method of claim 5, wherein the telephony service uses modulation.

7. (Original) The method of claim 6, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

8. (Original) The method of claim 1, wherein at least one of the first network device and the second network device is a mobile device.

9. (Original) The method of claim 8, wherein the mobile device is a notebook computer.

10. (Original) The method of claim 1, wherein the identifier associated with the second network device is a domain name.

11. (Original) The method of claim 1, the secure communication link supports data packets.

12. (Original) The method of claim 11, wherein the secure communication link is based on inserting into each data packet communicated over the secure communication link one or more data values that vary according to a pseudo-random sequence.

13. (Original) The method of claim 11, wherein communicating between the first and second network devices using the secure communications service via the secure communication link includes a network address hopping regime that is used to pseudo-randomly change network addresses in packets transmitted between the first network device and the second network device.

14. (Original) The method of claim 1, wherein determining that the second network device is available for a secure communications service is a function of a domain name lookup.

15. (Original) A system for connecting a first network device and a second network device, the system including one or more servers configured to:

receive, from the first network device, a request to look up a network address of the second network device based on an identifier associated with the second network device;

determine, in response to the request, whether the second network device is available for a secure communications service; and initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service,

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

16. (Original) The system of claim 15, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

17. (Original) The system of claim 15, wherein the secure communication link is a virtual private network communication link.

18. (Original) The system of claim 15, wherein the secure communications service includes a video conferencing service.

19. (Original) The system of claim 15, wherein the secure communications service includes a telephony service.

20. (Original) The system of claim 15, wherein the telephony service uses modulation.

21. (Original) The system of claim 20, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

22. (Original) The system of claim 15, wherein at least one of the first network device and the second network device is a mobile device.

23. (Original) The system of claim 22, wherein the mobile device is a notebook computer.

24. (Original) The system of claim 15, wherein the identifier associated with the second network device is a domain name.

25. (Original) The system of claim 15, wherein the secure communication link supports data packets.

26. (Original) The system of claim 25, wherein the secure communication link is based on inserting into each data packet communicated over the secure communication link one or more data values that vary according to a pseudo-random sequence.

27. (Original) The system of claim 25, wherein the secure communication link is based on a network address hopping regime that is used to pseudo-randomly change network addresses in packets transmitted between the first network device and the second network device.

28. (Original) The system of claim 15, wherein the determination that the second network device is available for the secure communications service is a function of the result of a domain name lookup.

REMARKS

Claims 1-28 remain in the application, of which Claims 1 and 15 are the independent claims. No claims have been amended or canceled. In the Office Action mailed July 30, 2012 ("Office Action"), claims 1-28 stand rejected under 35 U.S.C. § 103(a) based on U.S. Patent No. 5,898,830 ("*Wesinger*"). The rejections are traversed and reconsideration is respectfully requested in view of the following remarks.

Interview Summary

Applicants thank the Examiner for the courtesy extended to Applicants' representative Toby H. Kusmer, Reg. No. 26,418, during the personal interview conducted in the U.S. Patent and Trademark Office on August 23, 2012 ("first interview"), as well as to Toby H. Kusmer and Dr. Robert Short III at the personal interview conducted on October 18, 2012 ("second interview"). The Examiner mailed Interview Summaries on August 30, 2012, and October 18, 2012, summarizing certain aspects of the interviews. Applicants thank the Examiner for the Interview Summaries, and submit the following comments to address and clarify the Examiner's summary of those discussions.

During the first interview, Applicants' representative provided an overview of the claimed subject matter and discussed patentable distinctions of the claimed subject matter over the asserted reference, *Wesinger*. However, no agreement was reached regarding the allowability of the claims.

During the second interview, Applicants' representative and Dr. Short provided an overview of the claimed subject matter. Additionally, the Examiner, Applicants' representative, and Dr. Short discussed distinctions between the claimed subject matter and firewall systems such as in *Wesinger*. The Examiner suggested that one example feature discussed by Applicants' representative and Dr. Short during the interview – interception of a request to lookup a network address of a network device and a determination whether the network device is available for a secure communication service – was distinguishable over the prior art. The Examiner suggested that Applicants amend the claims accordingly.

In the second Interview Summary, the Examiner summarized the discussions of such allowable features as the "gist of the invention." Although Applicants agree that "interception of a request to look up a network address of a network device and a determination whether the network device is available for a secure communications service" is one feature that is distinguishable from the cited art, Applicants disagree with the second Interview Summary to the extent that it suggests that the above mentioned "intercepting" feature is the *only* novel and nonobvious aspect of Applicants' disclosed and/or claimed embodiments. Indeed, as discussed during the interview and described below, Applicants' disclosed and claimed embodiments include other novel and nonobvious aspects of the claimed subject matter. Other novel and unobvious aspects of the claimed subject include features that are found in the currently pending claims and in the claims presented prior to this Response. Thus, while Applicants appreciate the Examiner's suggestion to expedite allowance of this application, Applicants decline to amend the claims because they are already patentably distinguishable from *Wesinger* and other cited prior art, for at least the reasons below.

Claim Rejections – 35 U.S.C. § 103

To support an obvious rejection, "<u>all of the claim limitations</u> must be taught or suggested by the prior art applied and that <u>all words</u> in a claim must be considered in judging the patentability of that claim against the prior art." *Ex Parte Karl Burgess*, Appeal 2008-2820, 2009 WL 291172 (B.P.A.I. 2009), at *3 (citing *In re Royka*, 490 F.2d 981, 984-85 (CCPA 1974), *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970)) (emphasis added). A rejection based on obviousness "cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 126 S. Ct. 1727, 1741 (2007) (citing *In re Kahn*, 441 F.3d at 988). Here, the Office Action fails to demonstrate that each and every limitation of claims 1-28 are disclosed or suggested in *Wesinger*.

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

In *Wesinger*, "[w]hen a connection request is received, the firewall spawns a process, or execution thread, to create a virtual host VHn to handle that connection request." (*Id.* at 15:9-

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

Wesinger also discusses processing of DNS requests:

> When client C tries to initiate a connection to host D using the name of D, DNS operates in the usual manner to propagate a name request to successive levels of the network until D is found. The DNS server for D returns the network address of D to a virtual host on the firewall 155. The virtual host returns its network address to the virtual host on the firewall 157 from which it received the lookup request, and so on, until a virtual host on the firewall 105 returns its network address (instead of the network address of D) to the client C.

(*Id.* at 9:16-24.) Accordingly, when client C uses a name of D in a DNS request, C gets back an address for a virtual host of firewall 105, which faces C. (*See id.* at Fig. 1).

Wesinger describes processes and components different from the embodiments recited in claims 1-28. For example, independent claim 1 is representative and recites:

> A method of connecting a first network device and a second network device, the method comprising:
>
> receiving, from the first network device, a request to look up a network address of the second network device based on an identifier associated with the second network device;
>
> determining, in response to the request, whether the second network device is available for a secure communications service; and
>
> initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;
>
> wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Wesinger does not teach or suggest, for example, one or more servers that "***determining, in response to the request, whether the second network device is available for a secure communications service***." The Office action points to a portion of *Wesinger* that describes allowing or disallowing communications as corresponding to the claimed determination. (OA at 3 (citing *Wesinger* at 9:53-60).) That portion of *Wesinger*, however, does not demonstrate a server that determines, in response to the request, whether the second network device is available for a secure communications service. *Wesinger* describes that a firewall (a virtual host) checks parameters of the requested connection to determine whether the connection should be allowed. (*See Wesinger* at 9:53-60.) *Wesinger* does not demonstrate a server determining whether the second network device is "available," much less available for a secure communication service.

Wesinger briefly states that encryption may be used in combination with firewalls, but does not describe those firewalls as providing any determination of whether a second device is available for a secure communications service. (*See Wesinger* at 4:39-42; 12:22-28.) In fact, *Wesinger* describes that "[o]nce a connection has been allowed, the virtual host process invokes code that performs . . . channel processing (encryption . . .)." (*Id.* at 17:1-7.) Invoking code for encryption or the like *after a connection has already been established* does **not** teach or suggest *determining*, *in response to the request*, whether a second network device is *available* for a secure communications service.

Moreover, *Wesinger* does not teach or suggest initiating a VPN "***based on***" availability of the alleged second network device. *Wesinger* merely states that "[c]ombining encryption capabilities with programmable transparency . . . allows for the creation of virtual private networks," not that a VPN is initiated because of some determination. (*Id.* at 12:23-28.) *Wesinger*'s code that makes a connection transparent does not initiate a VPN based on any determination that the second network device is available. (*See*, *e.g.*, *Wesinger* at 4:39-42.)

Applicants also note that the Office Action does not specify which portions of *Wesinger* render obvious the feature of "the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device," as recited by claim 1. Indeed, *Wesinger* is not concerned with audio or video data. For at least that reason alone, a rejection based on *Wesinger* cannot be maintained. *KSR Int'l Co.*, 126 S. Ct. at 1741.

Accordingly, Applicants respectfully request that the rejection under 35 U.S.C. § 103 be withdrawn.

Independent claim 15, though of different scope from independent claim 1, recites similar features to those discussed above in connection with claim 1. Thus,for at least the explanations similar to those described above regarding independent claim 1, *Wesinger* is not understood to teach or suggest the features of independent claim 15. Since the cited references do not teach or suggest the features of claim 15, reconsideration and withdrawal of the rejection of independent claim 15 under § 103(a) are respectfully requested.

Claims 2-14 and 16-28 depend from claims 1 and 15, respectively. These dependent claims currently under consideration in the application are believed to be allowable for at least similar reasons to those discussed above with respect to claims 1 and 15. Additionally, dependent claims 2-14 and 16-28 are allowable for the additional reason that each of the claims recite additional features not disclosed or suggested by the cited references. Because each dependent claim is deemed to define an additional aspect of the invention, the individual consideration of each on its own merits is respectfully requested. Accordingly, reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

CONCLUSION

Applicants respectfully submit that all of the pending claims, claims 1-28, are in condition for allowance. Applicants respectfully invite the Examiner to contact the undersigned attorney to promptly address any questions or issues regarding the allowability of the pending claims.

Applicants' remarks in support of patentability of one claim should not be imputed to any other claim, even if similar terminology is used. Any absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because Applicants' remarks are not intended to be exhaustive, as there may be other reasons for patentability of any or all claims that have not been expressed. Finally, nothing in this response should be construed as an intent to concede any issue with regard to any claim, and the amendment or cancellation of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment or cancellation.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 502203 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: October 30, 2012

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Customer No. 23630
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile : (617)535-3800
E-mail: tkusmer@mwe.com

Kenneth C. Cheney, Reg. No. 61,841
4 Park Plaza
Suite 1700
Irvine, California 92614-2559
Telphone: (949) 757-7111
Facsimile: (949) 851-9348
E-mail: kcheney@mwe.com

Electronic Acknowledgement Receipt

EFS ID:	14107681
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	30-OCT-2012
Filing Date:	28-DEC-2011
Time Stamp:	20:41:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		077580_0154_VRNK-1CP3CNFT4_Reply_B.pdf	98661 e245ead1835a121f2f5f431a3154ab8518800f55	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	11

Warnings:

Information:

Total Files Size (in bytes):	98661

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/339,257	Filing Date 12/28/2011	☐ To be Mailed

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

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

APPLICATION AS AMENDED – PART II

AMENDMENT	10/30/2012	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 28	Minus	** 28	= 0	X $ =		OR	X $62=	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $250=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**0**

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

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

Legal Instrument Examiner:
/CORALIA BETANCOURT/

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	12/28/2011	Victor Larson	77580-154(VRNK-1CP3CNFT4)	1084

23630 7590 12/10/2012
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
12/10/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Office Action Summary	Application No.	Applicant(s)	
	13/339,257	LARSON ET AL.	
	Examiner	Art Unit	
	KRISNA LIM	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2012*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-28* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-28* is/are rejected.

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

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

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

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

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

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

4) ☐ Other: _____.

1. Claims 1-28 are still pending for examination.

2. The following is a quotation of 35 § U.S.C. 103 (a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1-28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wesinger [U.S. Patent No. 5,898,830].

4. Wesinger disclosed the invention substantially as claimed. Taking claims 1,2, 3, 1 O, 11, 12, 14, 15, 16, 17, 24, 25, 26, and 28 as exemplary claims, the reference disclose a method of connecting a first network device and a second network device (i.e., see Internet 120 of Fig. 1 connecting with other network devices), the method comprising:

receiving, from the first network device, a request to look up a network address of the second network device based on an identifier associated with the second network device (i.e. Wesinger disclosed at col. 8 (line 25) to col. 9 (line 25) " ... DNS is a ...

system that translates host name address to IP address and IP address to host name ... stored **in DNS tables** ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it **receives the look up request** ...”);

determining, in response to the request, whether the second network device is available for a secure communications service (i.e., Wesinger at col. 12 (lines 23-27) disclosed "... **combining encryption capabilities .... allows for the creation of virtual private networks-networks in which two remote machine communicate securely** ...", and at col. 8 (line 25) to col. 9 (line 25) Wesinger disclosed " ... DNS is a ... system that translates host name address to IP address and IP address to host name ... stored **in DNS tables** ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it **receives the look up request** ...”);

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service (i.e., Wesinger at col. 12 (lines 23-27) disclosed "... **combining encryption capabilities .... allows for the creation of virtual private networks-networks in which two remote machine communicate securely** ...", and at col. 8 (line 25) to col. 9 (line 25) Wesinger disclosed " ... DNS is a ... system that translates host name address to IP address and IP address to host name ... stored **in DNS tables** ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it **receives the look up request** ...”);

wherein the secure communication link is a virtual private network communication link and supports data packets (i.e., Wesinger at col. 12 (lines 23-27) disclosed "... **combining encryption capabilities .... allows for the creation of virtual private networks-networks in which two remote machine communicate securely** ...");

wherein the data is encrypted over the secure communication link (i.e., Wesinger at col. 12 (lines 23-27) disclosed "... **combining encryption capabilities ....**

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

wherein the determining of the second network device is available for a secure communications service is a function of a domain name look up (i.e. Wesinger disclosed at col. 8 (line 25) to col. 9 (line 25) " ... DNS is a ... system that translates host name address to IP address and IP address to host name ... stored **in DNS tables** ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it **receives the look up request** ...").

5. As to claims 4-9, and 18-23, those features (i.e., video data, audio data, video conference, telephone service using modulation based on FDM, TDM, or CDMA, mobile device, a notebook computer, etc.) are well known the art at the time the invention was made and they are not patentably distinguishable features.

6. As to claims 13 and 27, Wesinger further disclosed the steps of: establishing an IP address hopping scheme between the client and the target (i.e. col. 9, lines 7-25).

7. While Wesinger disclosed, at col. 9 (lines 16-25) the feature of "when a client C tries to <u>initiate a connection to host D </u>using the name D ... The DNS server for <u>D returns the network address of D </u>to a virtual host of the firewall 155. The virtual host <u>returns its network address </u>to the virtual host on the firewall 157 from which it <u>received the</u> lookup_ <u>request, </u>and so on, until a virtual host on the firewall 105 returns its network address (instead of the network address of D) to the client C", at col. 12 (lines 23-27) Wesinger further disclosed "... **combining encryption capabilities .... allows for the creation of virtual private networks-networks in which two remote machine communicate securely** ...", and at col. 8 (line 25) to col. 9 (line 25) Wesinger further disclosed " ... DNS is a ... system that translates host name address to IP address and IP address to host name ... stored **in DNS tables** ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it **receives the look up request** ..."), Wesinger did not mention as exactly as the

claimed language of "initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service". It would have been obvious to one of ordinary skill in the art to obviously recognize that Wesinger's passage above and the claimed language are obviously the same and the difference is how they are written which is obvious to one of ordinary skill in the art.

8. Applicant's arguments filed 10/30/2012 have been fully considered but they are not persuasive. In the remark, applicants argued that:

a) Wesinger does not disclose one or more servers that "determining in response to the request, whether the second network device is available for a secure communication service".

b) Wesinger does not disclose "initiating a VPN "based on" availability of the alleged second network device."

c) Wesinger does not disclose "the secure communication service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device".

9. As to paragraphs 8 a) to 8 c), Examiner respectfully disagrees because at paragraph 4 above Wesinger clearly disclosed those features. For example, Wesinger disclosed, at col. 9 (lines 16-25) the feature of "when a client C tries to initiate a connection to host D using the name D ... The DNS server for D returns the network address of D to a virtual host of the firewall 155. The virtual host returns its network address to the virtual host on the firewall 157 from which it received the lookup_ request, and so on, until a virtual host on the firewall 105 returns its network address (instead of the network address of D) to the client C", at col. 12 (lines 23-27) Wesinger further disclosed "... **combining encryption capabilities .... allows for the creation of virtual private networks-networks in which two remote machine communicate securely** ...", and at col. 8 (line 25) to col. 9 (line 25) Wesinger further disclosed " ... DNS is a ... system that translates host name address to IP address and IP address to

host name ... stored **in DNS tables** ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it **receives the look up request** ..."). Thus, it would have been obvious to one of ordinary skill in the art to recognize that Wesinger obviously taught the claimed language of "initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service". It would have been obvious to one of ordinary skill in the art to obviously recognize that Wesinger's passage above and the claimed language are obviously the same and the difference is how they are written which is obvious to one of ordinary skill in the art. Moreover, As to the specific data such as audio/video to be communicated between two devices are so well known in the art at the time the invention was made. And having audio/video to be communicated between two devices is not patentably distinguishable feature.

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

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956 The examiner can normally be reached on Tuesday to Friday from 7:10 AM to 5:40 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele, can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (In USA or Canada) or 571-272-100.

Kl
December 01, 2012

/Krisna Lim/
Primary Examiner Art Unit 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1213	Extended European Search Report dated 03/26/12 from Corresponding European Application Number 11005793.2 (077580-0144)	
	D1214	Bergadano, et al., "Secure WWW Transactions Using Standard HTTP and Java Applets," Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998	

EXAMINER /Krisna Lim/	DATE CONSIDERED 12/01/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	**13/339,257**
				Filing Date	**12-28-2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Krisna Lim**
				Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Date: 7/24/12

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

DM_US 36888499-1.077580.0154

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1220	Defendants' Motion For Reconsideration of the Construction of the Term "Secure Communication Link," 7 pages, June 2012	
	D1221	Green, "Cisco Leverages Altiga Technology for VPN's," 2 pages, 2000 http://www.crn.com/news/channel-programs/18807923/cisco-leverages-altiga-technology-for-vpns.htm	
	D1222	Altiga Networks Archived at http://web.archive.org/web/20000823023437/http:/www.altiga.com/products/ 1999 and Retrieved by the Wayback Machine	
	D1223	Kiuchi, "C-HTTP The Development of a Secure, Closed HTTP-Based Network on the Internet," Department of Epidemiology and Biostatistics, Faculty of Medicine, University of Tokyo, Japan	

EXAMINER /Krisna Lim/	DATE CONSIDERED 12/01/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Date: 9/24/12

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

DM_US 38997101-1.077580.0154

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1224	Lee et al., "Uniform Resource Locators (URL)," Network Working Group, RFC 1738, , December 1994 (25 pages)	
	D1225	VPN 3000 Concentrator Series, User Guide; Release 2.5 July 2000 (489 pages)	
	D1226	VPN 3000 Concentrator Series, Getting Started; Release 2.5 July 2000 (122 pages)	
	D1227	Fratto, Altiga Concentrates on VPN Security (Hardware Review Evaluation), Network Computing, March 22, 1999 (2 pages)	
	D1228	Response to RFP: Altiga, Network World Fusion, May 10, 1999 (7 pages)	
	D1229	Altiga Proves Multi-Vendor Interoperability for Seamless VPN Deployment; VPN Workshop Marks Significant Development in the VPN Market, July 12, 1999 (2 pages)	
	D1230	Altiga VPN Concentrator Series (C50) Versus Nortel Networks Contivity Extranet Switch 4000 and 4500, VPN Tunneling competitive Evaluation, 1999 (6 pages)	
	D1231	VPN 3000 Client User Guide, Release 2.5, July 2000 (94 pages)	
	D1232	Digital Certificates Design Specification for Release 2.0, May 17, 1999 (21 pages)	
	D1233	Altiga IPSec Client Architecture, Revision 1.0, April 5, 1999 (34 pages)	
	D1234	Altiga IPSec Functional Specification, Revision 2.1, (17 pages)	
	D1235	Altiga Product Requirements, Revision 1.7, May 26, 1998 (17 pages)	
	D1236	Altiga Network Lists Feature Functional Specification, Revision 1.0, (7 pages)	
	D1237	Altiga Split Tunneling Functional/Design Specification, (15 pages)	

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1238	Altiga Digital Certificate Support for IPSec Client V2.1 Functional Specification, August 12, 1999 (24 pages)	
	D1239	Altiga IPSec LAN to LAN Tunnel Autodiscovery Functional Specification, (5 pages)	
	D1240	Altiga Split Tunneling Testplan, Revision 1.0, (8 pages)	
	D1241	Altiga VPN Concentrator Getting Started, Revision 1, March 1999 (116 pages)	
	D1242	Altiga VPN Concentrator Getting Started, Version 2, June 1999 (102 pages)	
	D1243	Altiga VPN Concentrator Getting Started, Version 3, December 1999 (130 pages)	
	D1244	Altiga VPN Concentrator Getting Started, Version 4, March 2000 (138 pages)	
	D1245	Altiga VPN Concentrator User Guide, Revision 1, March 1999 (304 pages)	
	D1246	Altiga VPN Concentrator User Guide, Revision 1.1, March 1999 (304 pages)	
	D1247	Altiga VPN Concentrator User Guide, Version 3, June 1999 (478 pages)	
	D1248	Altiga VPN Concentrator User Guide, Version 4, December 1999 (472 pages)	
	D1249	Altiga VPN Concentrator User Guide, Version 5, March 2000 (606 pages)	
	D1250	Altiga VPN Client Installation and User Guide, Version 2, July 1999 (92 pages)	
	D1251	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 3, December 1999 (113 pages)	
	D1252	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 4, March 2000 (118 pages)	
	D1253	Altiga Networks VPN Concentrator and VPN Client, as well as their Public Demonstrations and Testing, are also Described in Marketing Materials and Publications (4 pages)	

EXAMINER /Krisna Lim/	DATE CONSIDERED 12/01/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby H Kusmer

Date: 10/3/12

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

DM_US 39145292-1.077580.0154

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1215	Alexander Invalidity Expert Report dtd May 22, 2012 with Exhibits	
	D1216	Deposition of Peter Alexander dtd July 27, 2012	
	D1217	Cisco '151 Comments by Third Party Requester dtd August 17, 2012 with Exhibits	
	D1218	Cisco '151 Petition to Waive Page Limit Requirement for Third Party Comments dtd August 17, 2012	
	D1219	Deposition of Stuart Stubblebine dtd August 22, 2012	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	12/01/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

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

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Hasan M. Rashid

Date: 8/27/12

Hasan M. Rashid; Reg. No.:62,390
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 37791246-1.077580.0154

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

Index of Claims	Application/Control No. 13339257	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	02/25/2012	07/18/2012	12/01/2012						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21	✓	✓	✓						
	22	✓	✓	✓						
	23	✓	✓	✓						
	24	✓	✓	✓						
	25	✓	✓	✓						
	26	✓	✓	✓						
	27	✓	✓	✓						
	28	✓	✓	✓						

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson, *et al.*	:	
	:	
Serial No.: 13/339,257	:	Confirmation No. 1084
	:	
Filed: December 28, 2011	:	Group Art Unit: 2453
	:	
Customer Number: 23630		Examiner: Lim, Krisna

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

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

AMENDMENT AFTER FINAL REJECTION
UNDER 37 CFR § 1.116

Dear Commissioner:

This Reply is being filed in response to the Final Office Action mailed from the United States Patent and Trademark office on December 10, 2012. Pursuant to 37 C.F.R. § 1.116, Applicants propose that this application be amended as follows:

Amendment to the Claims begin on page 2 of this paper.

Remarks begin on page 6 of this paper.

IN THE CLAIMS

Applicants propose that this listing of the claims replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method of connecting a first network device and a second network device, the method comprising:

    intercepting, ~~receiving,~~ from the first network device, a request to look up an internet protocol (IP) ~~a network~~ address of the second network device based on a domain name ~~an identifier~~ associated with the second network device;

    determining, in response to the request, whether the second network device is available for a secure communications service; and

    initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

    wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

2. (Original) The method of claim 1, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

3. (Original) The method of claim 1, wherein the secure communication link is a virtual private network communication link.

4. (Original) The method of claim 1, wherein the secure communications service includes a video conferencing service.

5. (Original) The method of claim 1, wherein the secure communications service includes a telephony service.

6. (Original) The method of claim 5, wherein the telephony service uses modulation.

7. (Original) The method of claim 6, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

8. (Original) The method of claim 1, wherein at least one of the first network device and the second network device is a mobile device.

9. (Original) The method of claim 8, wherein the mobile device is a notebook computer.

10. (Canceled)

11. (Currently Amended) The method of claim 1, wherein the secure communication link supports data packets.

12. (Original) The method of claim 11, wherein the secure communication link is based on inserting into each data packet communicated over the secure communication link one or more data values that vary according to a pseudo-random sequence.

13. (Original) The method of claim 11, wherein communicating between the first and second network devices using the secure communications service via the secure communication link includes a network address hopping regime that is used to pseudo-randomly change network addresses in packets transmitted between the first network device and the second network device.

14. (Original) The method of claim 1, wherein determining that the second network device is available for a secure communications service is a function of a domain name lookup.

15. (Currently Amended) A system for connecting a first network device and a second network device, the system including one or more servers configured to:

intercept, ~~receive,~~ from the first network device, a request to look up an internet protocol (IP) ~~a network~~ address of the second network device based on a domain name ~~an identifier~~ associated with the second network device;

determine, in response to the request, whether the second network device is available for a secure communications service; and initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service,

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

16. (Original) The system of claim 15, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

17. (Original) The system of claim 15, wherein the secure communication link is a virtual private network communication link.

18. (Original) The system of claim 15, wherein the secure communications service includes a video conferencing service.

19. (Original) The system of claim 15, wherein the secure communications service includes a telephony service.

20. (Original) The system of claim 15, wherein the telephony service uses modulation.

21. (Original) The system of claim 20, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

22. (Original) The system of claim 15, wherein at least one of the first network device and the second network device is a mobile device.

23. (Original) The system of claim 22, wherein the mobile device is a notebook computer.

24. (Canceled)

25. (Original) The system of claim 15, wherein the secure communication link supports data packets.

26. (Original) The system of claim 25, wherein the secure communication link is based on inserting into each data packet communicated over the secure communication link one or more data values that vary according to a pseudo-random sequence.

27. (Original) The system of claim 25, wherein the secure communication link is based on a network address hopping regime that is used to pseudo-randomly change network addresses in packets transmitted between the first network device and the second network device.

28. (Original) The system of claim 15, wherein the determination that the second network device is available for the secure communications service is a function of the result of a domain name lookup.

29. (New) The method of claim 1, wherein intercepting the request consists of receiving the request to determine whether the second network device is available for the secure communications service.

30. (New) The system of claim 15, wherein the one or more servers are configured to intercept the request by receiving the request to determine whether the second network device is available for the secure communications service.

31. (New) The method of claim 1, wherein intercepting the request occurs within another network device that is separate from the first network device.

32. (New) The system of claim 15, wherein the one or more servers configured to intercept the request are separate from the first network device.

REMARKS

Claims 1-9, 11-23, and 25-32 are pending in this application, of which Claims 1 and 15 are the independent claims. By this Amendment, Applicants propose to amend independent claims 1 and 15 and dependent claim 11, add new dependent claims 29-32, and cancel claims 10 and 24 without prejudice or disclaimer of the subject matter thereof. [1]

Summary of Telephone Interview

Applicants appreciate the courtesies extended to Applicants' undersigned representative during the informal telephone interview conducted on February 20, 2013. During the interview, Applicants' representative proposed amending the independent claims as set forth in this Amendment. The Examiner agreed that he would enter the Amendment and allow the claims if Applicants amended the claims as proposed in this Amendment.

Claim Rejections – 35 U.S.C. § 103

The December 10, 2012, Final Office Action rejects claims 1-28 under 35 U.S.C. § 103(a) based on U.S. Patent No. 5,898,830 ("*Wesinger*"). The rejection of canceled claims 10 and 24 is moot. Applicants respectfully traverse the rejection of the remaining claims. For at least the reasons discussed in the October 30, 2012 Response, *Wesinger* does not disclose or suggest the features recited in independent claims 1 and 15, which are therefore allowable over *Wesinger*.

Moreover, as discussed above, the Examiner agreed during the February 20, 2013, telephone interview that he would withdraw the rejection in view of *Wesinger* and allow the pending claims, provided that Applicants amend the independent claims as Applicants propose to amend them by this Amendment. Thus, while Applicants maintain that the original claims presented on December 28, 2011 distinguish over *Wesinger*, Applicants amend the claims as listed above solely to expedite prosecution of this application.

---

[1] Applicants disagree that the original claims submitted on December 28, 2011 are disclosed or obvious over the prior art. However, Applicants amend the claims to expedite prosecution of this matter as explained in this Amendment. Applicants reserve the right to pursue patent protection for the embodiments recited in the original claims and variants thereof, in one or more continuation applications.

In view of the above, the rejection of independent claims 1 and 15 should be withdrawn and the claims should be allowed. Moreover, each pending dependent claim ultimately depends from one of independent claims 1 and 15 and is therefore allowable based on its dependency from an allowable base claim as well as for reciting additional features. Accordingly, Applicants respectfully request that the Examiner enter this Amendment under 37 C.F.R. § 1.116, withdraw the § 103 rejection, and place claims 1-9, 11-23, and 25-32 in condition for allowance.

Applicants submit that the proposed amendments of claims 1, 11, and 15 and the proposed addition of dependent claims 29-32 do not raise new issues or necessitate the undertaking of any additional search of the art by the Examiner. Therefore, this Amendment should allow for immediate action by the Examiner. Furthermore, Applicants respectfully submit that the entry of the Amendment would place the application in condition for allowance, as indicated by the Examiner during the telephone interview. Finally, Applicants submit that the entry of the Amendment would place the application in better form for appeal, should the Examiner dispute the patentability of the pending claims.

CONCLUSION

Applicants respectfully submit that all of the pending claims, claims 1-9, 11-23, and 25-32, are in condition for allowance. If any questions remain, or should the present response not place the claims in condition for allowance, the Examiner is cordially invited to contact the undersigned attorney so that any such matters may be promptly resolved.

Any remarks in support of patentability of one claim should not be imputed to any other claim, even if similar terminology is used. Any remarks referring to only a portion of a claim should not be understood to base patentability on that portion; rather, patentability rests on each claim taken as a whole. The absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be other reasons for patentability of any or all claims that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment or cancellation of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment or cancellation.

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

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: February 27, 2013

/Toby H. Kusmer/

Toby H. Kusmer, P.C., Reg. No. 26,418
Customer No. 23630
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile : (617)535-3800
E-mail: tkusmer@mwe.com

DM_US 41322676-1.077580.0154

Electronic Patent Application Fee Transmittal

Application Number:	13339257
Filing Date:	28-Dec-2011
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kimila Carraway
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in Excess of 20	1202	2	62	124
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**124**

Electronic Acknowledgement Receipt

EFS ID:	15070473
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	27-FEB-2013
Filing Date:	28-DEC-2011
Time Stamp:	20:12:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$124
RAM confirmation Number	10261
Deposit Account	501133
Authorized User	

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

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

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

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		077580-0154_Amendment_After_Final.pdf	51496 8fdb7278860cdf6c8ba17364a8cedb44602d556b	yes	8

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment After Final	1	1
Claims	2	5
Applicant Arguments/Remarks Made in an Amendment	6	8

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30739 ea0e0defb25e974989e8352e791124a53ff2a1fe	no	2

Warnings:

Information:

Total Files Size (in bytes): 82235

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/339,257	Filing Date 12/28/2011	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

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

APPLICATION AS AMENDED – PART II

AMENDMENT		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	02/27/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 30	Minus	** 28	= 2	X $ =		OR	X $62=	124
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $250=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**124**

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

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

Legal Instrument Examiner:
/BRENDA J. DENNY/

US006502135C1

(12) INTER PARTES REEXAMINATION CERTIFICATE (0271st)

United States Patent (10) **Number:** **US 6,502,135 C1**
Munger et al. (45) **Certificate Issued:** **Jun. 7, 2011**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY**

(75) Inventors: **Edmund Colby Munger**, Crownsville, MD (US); **Douglas Charles Schmidt**, Severna Park, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

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

Reexamination Request:
No. 95/001,269, Dec. 8, 2009

Reexamination Certificate for:

Patent No.:	**6,502,135**
Issued:	**Dec. 31, 2002**
Appl. No.:	**09/504,783**
Filed:	**Feb. 15, 2000**

Certificate of Correction issued Sep. 9, 2003.

Related U.S. Application Data

(63) Continuation 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.** **709/225**; 709/229; 709/245

(58) **Field of Classification Search** 709/225
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502 A	7/1959	Roper et al.
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

(Continued)

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

(Continued)

OTHER PUBLICATIONS

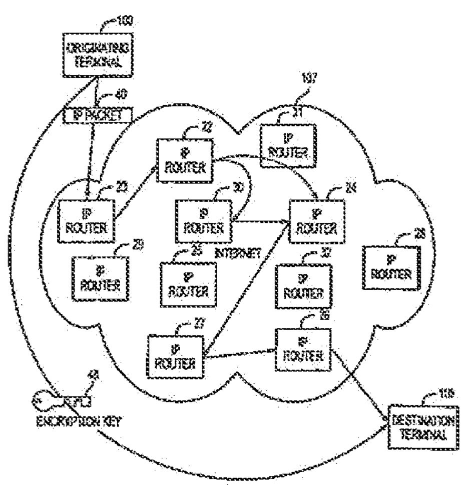
Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/draft302.txt on Feb. 4, 2002, 56 pages.

(Continued)

Primary Examiner—Andrew L Nalven

(57) **ABSTRACT**

A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design include (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities.



U.S. PATENT DOCUMENTS

5,311,593	A	5/1994	Carmi
5,329,521	A	7/1994	Walsh et al.
5,341,426	A	8/1994	Barney et al.
5,367,643	A	11/1994	Chang et al.
5,384,848	A	1/1995	Kikuchi
5,511,122	A	4/1996	Atkinson
5,559,883	A	9/1996	Williams
5,561,669	A	10/1996	Lenney et al.
5,588,060	A	12/1996	Aziz
5,625,626	A	4/1997	Umekita
5,629,984	A	5/1997	McManis
5,654,695	A	8/1997	Olnowich et al.
5,682,480	A	10/1997	Nakagawa
5,689,566	A	11/1997	Nguyen
5,740,375	A	4/1998	Dunne et al.
5,764,906	A	6/1998	Edelstein et al.
5,771,239	A	6/1998	Moroney et al.
5,774,660	A	6/1998	Brendel et al.
5,787,172	A	7/1998	Arnold
5,796,942	A	8/1998	Esbensen
5,805,801	A	9/1998	Holloway et al.
5,805,803	A	9/1998	Birrell et al.
5,822,434	A	10/1998	Caronni et al.
5,842,040	A	11/1998	Hughes et al.
5,845,091	A	12/1998	Dunne et al.
5,864,666	A	1/1999	Shrader
5,867,650	A	2/1999	Osterman
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 et al.
5,905,859	A	5/1999	Holloway et al.
5,918,019	A	6/1999	Valencia
5,950,195	A	9/1999	Stockwell et al.
5,996,016	A	11/1999	Thalheimer et al.
6,006,259	A	12/1999	Adelman et al.
6,006,272	A	12/1999	Aravamudan et al.
6,016,318	A	1/2000	Tomoike
6,016,512	A	1/2000	Huitema
6,041,342	A	3/2000	Yamaguchi
6,052,788	A	4/2000	Wesinger et al.
6,055,574	A	4/2000	Smorodinsky et al.
6,061,346	A	5/2000	Nordman
6,061,736	A	5/2000	Rochberger et al.
6,079,020	A	6/2000	Liu
6,081,900	A	6/2000	Subramaniam et al.
6,092,200	A	7/2000	Muniyappa et al.
6,101,182	A	8/2000	Sistanizadeh et al.
6,119,171	A	9/2000	Alkhatib
6,119,234	A	9/2000	Aziz et al.
6,147,976	A	11/2000	Shand et al.
6,157,957	A	12/2000	Berthaud
6,158,011	A	12/2000	Chen et al.
6,168,409	B1	1/2001	Fare
6,173,399	B1	1/2001	Gilbrech
6,175,867	B1	1/2001	Taghadoss
6,178,409	B1	1/2001	Weber et al.
6,178,505	B1	1/2001	Schneider et al.
6,179,102	B1	1/2001	Weber et al.
6,199,112	B1	3/2001	Wilson
6,202,081	B1	3/2001	Naudus
6,222,842	B1	4/2001	Sasyan et al.
6,223,287	B1	4/2001	Douglas et al.
6,226,748	B1	5/2001	Bots et al.
6,226,751	B1	5/2001	Arrow et al.
6,233,618	B1	5/2001	Shannon
6,243,360	B1	6/2001	Basilico
6,243,749	B1	6/2001	Sitaraman et al.
6,243,754	B1	6/2001	Guerin et al.
6,246,670	B1	6/2001	Karlsson et al.
6,256,671	B1	7/2001	Strentzsch et al.
6,262,987	B1	7/2001	Mogul
6,263,445	B1	7/2001	Blumenau
6,286,047	B1	9/2001	Ramanathan et al.
6,298,341	B1	10/2001	Mann et al.
6,301,223	B1	10/2001	Hrastar et al.
6,308,274	B1	10/2001	Swift
6,311,207	B1	10/2001	Mighdoll et al.
6,314,463	B1	11/2001	Abbott et al.
6,324,161	B1	11/2001	Kirch
6,330,562	B1	12/2001	Boden et al.
6,332,158	B1	12/2001	Risley et al.
6,333,272	B1	12/2001	McMillin et al.
6,338,082	B1	1/2002	Schneider
6,353,614	B1	3/2002	Borella et al.
6,430,155	B1	8/2002	Davie et al.
6,430,610	B1	8/2002	Carter
6,487,598	B1	11/2002	Valencia
6,502,135	B1	12/2002	Munger et al.
6,505,232	B1	1/2003	Mighdoll et al.
6,510,154	B1	1/2003	Mayes et al.
6,549,516	B1	4/2003	Albert et al.
6,557,037	B1	4/2003	Provino
6,571,296	B1	5/2003	Dillon
6,571,338	B1	5/2003	Shaio et al.
6,581,166	B1	6/2003	Hirst et al.
6,618,761	B2	9/2003	Munger et al.
6,671,702	B2	12/2003	Kruglikov et al.
6,687,551	B2	2/2004	Steindl
6,687,746	B1	2/2004	Shuster et al.
6,701,437	B1	3/2004	Hoke et al.
6,714,970	B1	3/2004	Fiveash et al.
6,717,949	B1	4/2004	Boden et al.
6,752,166	B2	6/2004	Lull et al.
6,757,740	B1	6/2004	Parekh et al.
6,760,766	B1	7/2004	Sahlqvist
6,826,616	B2	11/2004	Larson et al.
6,839,759	B2	1/2005	Larson et al.
6,937,597	B1	8/2005	Rosenberg et al.
7,010,604	B1	3/2006	Munger et al.
7,039,713	B1	5/2006	Van Gunter et al.
7,072,964	B1	7/2006	Whittle et al.
7,133,930	B2	11/2006	Munger et al.
7,167,904	B1	1/2007	Devarajan et al.
7,188,175	B1	3/2007	McKeeth
7,188,180	B2	3/2007	Larson et al.
7,197,563	B2	3/2007	Sheymov et al.
7,353,841	B2	4/2008	Kono et al.
7,461,334	B1	12/2008	Lu et al.
7,490,151	B2	2/2009	Munger et al.
7,493,403	B2	2/2009	Shull et al.
2001/0049741	A1	12/2001	Skene et al.
2002/0004898	A1	1/2002	Droge
2004/0199493	A1	10/2004	Ruiz et al.
2004/0199520	A1	10/2004	Ruiz et al.
2004/0199608	A1	10/2004	Rechterman et al.
2004/0199620	A1	10/2004	Ruiz et al.
2005/0055306	A1	3/2005	Miller et al.
2007/0208869	A1	9/2007	Adelman et al.
2007/0214284	A1	9/2007	King et al.
2007/0266141	A1	11/2007	Norton
2008/0235507	A1	9/2008	Ishikawa et al.

FOREIGN PATENT DOCUMENTS

GB	2 317 792	4/1998
GB	2 334 181 A	8/1999
JP	62-214744	9/1987
JP	04-363941	12/1992
JP	09-018492	1/1997
JP	10-070531	3/1998
WO	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 00/17775	3/2000
WO	WO 001/17775	3/2000
WO	WO 00/70458	11/2000
WO	WO 01/016766	3/2001
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

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 Abstact), 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 (dataed 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.

Sankar, 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.

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).

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 Uezona, "Network Security", Japan, Nikkei McGraw–Hill, Dec. 5, 1958, First Edition, first copy, p. 102–108.

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 corresponding 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. 5, 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? 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.

Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX).

Automative 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/sockswp.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 1998 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 NewOpportunities 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 IPSecurity*, <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 8 Assurance Computer Systems (Jun. 2, 1997). (Syverson, Onion Routing).

Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG 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 hap //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/TULARC/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, 45 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 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 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail).

Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail Administrator 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, *Linux 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). (Bhattcharya 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 ANX 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).

Publically 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).

Darrell 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.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-insuit).

Microsoft Corp. Windows NT Servier Product Documentation: Administration Kit Guide—Connection Manager, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.).

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 (Cariplo I).

Marc Levy, COM Internet Services (Apr. 23, 1999), available at 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 (Horstmann).

Microsoft Corp., DCOM: A Business Overview (Apr. 1997), available at 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 (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 (Suhy).

126. Aaron Skonnard, *Essential Winlnet* 313–423 (Addison Wesley Longman 1998) (Essential Winlnet).

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).

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).

Microsoft Corp. Internet Connection Services for RAS, Commercial Edition, available athttp://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (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.mspx (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 Verion 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.mspx (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 (Remote Access).

Microsoft Corp., Understanding PPTP (Windows NT 4.0), available at http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.).

Microsoft Corp., Windows NT 4.0: Virtual Private Networking, available at http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.).

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/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13.

Microsoft Corp., Windows NT Server Product Documentation: Chapter 5—Planning for Large-Scale Configurations, available at http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.).

F-Secure, F-Secure Evaluation Kit (May 1999) (FSECURE 00000003) (Evaluation Kit 3).

F-Secure, F-Secure NameSurfer (May 1999) (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) (F-secure 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) (F-secure 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).

VX00088640

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: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technical 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 Releaset Notes* (Jul. 21, 2000).
Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106* (Contract No. F30602-98-C-0012) (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, *Informatiion 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 (Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft 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/book/id_762/viewer_r.asp?bookid=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/19970620031945/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.

E-mails 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," Networking 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 with ESP and AH," RFC 2404 (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 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. 7,188,180, dated Nov. 25, 2009.

Exhibit 2 "Aventail Connect v3.1/v2.6 Administrator's Guide", 120 pages, 1996-1999.

Exhibit 3A, "Gauntlet Firewall for Windows", pp. 1-137, 1998-1999.

Exhibit 3B, "Gauntlet Firewall for Windows", pp. 138-275, 1998-1999.

Exhibit 4, "Kosiur", Building and Managing VPNs, pp. 1-396, 1998.

Exhibit 5, Building a Microsoft VPN; A comprehensive Collection of Microfoft Resources, pp. 1-216.

Exhibit 6, Windows NT Server, Virtual Private Network; An Overview, pp. 1-26, 1998.

Exhibit 7, "Networking Working Group Request for Comments: 1035" pp. 1-56, 1987.

1

INTER PARTES REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 316

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1-10** and **12** is confirmed.

New claim **18** is added and determined to be patentable.

Claims **11** and **13-17** were not reexamined.

18. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

2

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer, wherein:

steps (2) and (3) are performed at a DNS server separate from the client computer, and step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request.

* * * * *

VX00088643

Electronic Acknowledgement Receipt

EFS ID:	15102825
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	04-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	11:54:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1397.pdf	60279 358af2f1b62d3f83c602d5f407fa093ec52937f3	no	2

Warnings:

Information:

2	Non Patent Literature	D1398part1.pdf	3822723 5952bf305ba0da87ebd8431548e57eb6ae949c48	no	110

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

3	Non Patent Literature	D1398part2.pdf	3139798 3286bc3d9b690cf8c69a778d495e2eec5b7e27bf	no	69

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

4	Non Patent Literature	D1399.pdf	333444 1ae45dff836983327845782475b139131ddd6853	no	6

Warnings:

Information:

5	Non Patent Literature	D1400.pdf	285807 d2efb93ba54c5467fcaf4801bdd81ce569b8aca4	no	7

Warnings:

Information:

6	Non Patent Literature	D1401.pdf	253888 ce6544195e609f1f578a1f6c5e0a8a0b80cc2eee	no	4

Warnings:

Information:

7	Non Patent Literature	D1402.pdf	14554816 8320fb13ad91d6d5e87cb660e6684d4a7558b5b3	no	64

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

8	Non Patent Literature	D1403.pdf	5321642 30c73b64ca748696c3217bc2c0eab3496f58d686	no	10

Warnings:

Information:

9	Non Patent Literature	D1404.pdf	958313 7ca7fed5177010a3b42769b111b2f7558c2c43f7	no	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:					
10	Non Patent Literature	D1405.pdf	116396 eaeec236192eecc32d9cf306d2563942aa37 5926	no	2
Warnings:					
Information:					
11	Non Patent Literature	D1406.pdf	1483724 8f4bd461e0b2df6b3aa6ba4cfcdeff73b15d aaa5	no	18
Warnings:					
Information:					
12	Non Patent Literature	D1407.pdf	2439641 d88eca147829a3c5039a46b2c0e63e00d6e fdca3	no	37
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
13	Non Patent Literature	D1408.pdf	1969680 c4e9f131b17b976f7512f0a8ff5ec0413c08f 460	no	24
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
14	Non Patent Literature	D1409.pdf	184126 748e7c68d71553217eaa4ba6ee615a58255 8c95c	no	14
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
15	Non Patent Literature	D1410.pdf	240704 9b1e5bc837ef6cd09ee58bcc4ef16be5d62f 249d	no	3
Warnings:					
Information:					
16	Non Patent Literature	D1411.pdf	1246690 8f56d4c2bbb422c0696dd9a42c8390b8331 169d5	no	12
Warnings:					
Information:					

17	Non Patent Literature	D1412.pdf	371629 702ab63954ec638403ee41f30cc00dde5b241fa7	no	4

Warnings:

Information:

Total Files Size (in bytes):	36783300

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Acknowledgement Receipt

EFS ID:	15096032
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	04-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	11:48:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1277.pdf	6592950 bf2f5e7e664399d90f8c8da0db5a6c6331072f91	no	154

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2	Non Patent Literature	D1278.pdf	7384245 661f70d16db974409d7840194049f9c522082c0b	no	163

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

3	Non Patent Literature	D1279.pdf	6257208 b2830e53df4ca72e2c1d8844d8f95516f878ca1f	no	141

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

4	Non Patent Literature	D1280.pdf	3705608 8ce24f484faec3da2707a6f375682fd491bf241b	no	181

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

5	Non Patent Literature	D1281.pdf	7982752 c9033342ba1e9325ee97570ee7318936fdc8f975	no	198

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

6	Non Patent Literature	D1282.pdf	3126761 47e08f5ed556192529173e50275d195e404eb754	no	154

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

7	Non Patent Literature	D1283.pdf	6751957 a06cab3d42a48f3bff347a87380784d8ddf1137d	no	143

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

8	Non Patent Literature	D1284.pdf	2294406 e6584bf29f618249c85415ecddb44e7d720e9cc8	no	122
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
9	Non Patent Literature	D1285.pdf	3776611 bd7fade1aba0c2ace33109586bd370073f28b4f6	no	153
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	Non Patent Literature	D1286.pdf	3271886 f1c5c1a830edf1e846183e073ae459be64064272	no	169
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
11	Non Patent Literature	D1287part1.pdf	6768328 3e5e65c04681d43597906f7720d3ec4532f3f84d	no	150
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
12	Non Patent Literature	D1287part2.pdf	25754832 14bc3a6939f02ab95128db5c7546f4fc2a4486dd	no	80
Warnings:					
Information:					
13	Non Patent Literature	D1288.pdf	2677956 90995c694458618236a61b0eb9ea4b225d9063ed	no	98
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
14	Non Patent Literature	D1289.pdf	315608 d4bc9cad5476c3378890fe919d210e85c1b82d08	no	12
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					

Information:

15	Non Patent Literature	D1290.pdf	1190467 761affb6394261888853f2f445d4710c0ed7 866c	no	26

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

16	Non Patent Literature	D1291.pdf	1151230 2da3b15e0c77faf8f57601ba92c5f57e52d8 83b1	no	26

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

17	Non Patent Literature	D1292.pdf	922465 7dc424353d785b3335d98a14a66adcb428 636402	no	24

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

18	Non Patent Literature	D1293.pdf	770990 9d5192029566db32fdaf39bca241c6a7ab1 ab2c3	no	24

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

19	Non Patent Literature	D1294.pdf	3507569 4cf13095dff5a221b23ca701ed53a58f1139 59c8	no	91

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

20	Non Patent Literature	D1295.pdf	2687595 0dea30cb6abe860acd764c0e12048643aec 87ec1	no	90

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

21	Non Patent Literature	D1296.pdf	511028 fe8d7387a99508be8688db7928771991728 0f310	no	20

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

22	Non Patent Literature	D1297.pdf	2332363 38a47893a308cca003d3488836163a3592a1c6a8	no	60

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

23	Non Patent Literature	D1298.pdf	752172 175f607189f50b479afdf7a5c1d50766c2e0f470	no	22

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

24	Non Patent Literature	D1299.pdf	133438 1ae1b6cc7e12a7312402a8cc850f90f84640bb1e	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:

25	Non Patent Literature	D1300.pdf	48832 3f906defd2803d69b023ecfdb551acbf26c8d812	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:

26	Non Patent Literature	D1301.pdf	45690 d2e5f60a19fbc1ceace8bd39d4fa0f71ceaa532d	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:

27	Non Patent Literature	D1302.pdf	784759 78c9d93d3cdb05b02805533a621b3dbe14711d86	no	22

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

28	Non Patent Literature	D1303.pdf	216797 0c3e4af15c8395140bc4e9277fbd69ab7b8a67a2	no	6
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
29	Non Patent Literature	D1304.pdf	14927871 15a355991d728993517819547b2af81fdda52eb1	no	184
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
30	Non Patent Literature	D1305.pdf	1639377 3f2ee4e30b0d8277286c9589d857a6ed57179850	no	3
Warnings:					
Information:					
31	Non Patent Literature	D1306.pdf	16823 fcf22d37e6aac1bf540589be71f39d16fca80a6f	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:					
32	Non Patent Literature	D1307.pdf	101465 b3d16dea228f461c03f1f5436f14cfb74b3122b5	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:					
33	Non Patent Literature	D1308.pdf	1713912 5d3b52c468d964a44056235ce0f19346b43bdfa1	no	3
Warnings:					
Information:					
34	Non Patent Literature	D1309.pdf	4837212 71cd505e05ee38db05e0c80e55c42915f07d2254	no	26
Warnings:					
Information:					

35	Non Patent Literature	D1310.pdf	1726922 f687bf9fc6f27805c1db848b7fb02ff172cbe eb1	no	3

Warnings:

Information:

36	Non Patent Literature	D1311.pdf	401591 11973f6357e29088a2eb474659dc28eae64 9e1a2	no	6

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

37	Non Patent Literature	D1312.pdf	2108729 451d9ff1453b51f9c61d46baed16e6fce3e7 523c	no	5

Warnings:

Information:

38	Non Patent Literature	D1313.pdf	63776 6821b85fea68253b4b9cdb3204b7f32aab9 a57d9	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:

39	Non Patent Literature	D1314.pdf	1542980 31b4f75f9eeea7ddd051716ba894e2be65b 2ac05	no	2

Warnings:

Information:

40	Non Patent Literature	D1315.pdf	1329379 b2ec3b27189c0fe0de9d1c4718c1df4190ce 4120	no	2

Warnings:

Information:

41	Non Patent Literature	D1316.pdf	623682 94076e48f82f7eccae0329b5dab209050dd 2b73f	no	11

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

42	Non Patent Literature	D1317.pdf	2160424 e924afcfef661b92945145fba4a6c94bcc15f 7a2	no	4

Warnings:

Information:					
43	Non Patent Literature	D1318.pdf	2036652 2766ec5cf4861facd5686a94d55974010394c648	no	8
Warnings:					
Information:					
44	Non Patent Literature	D1319.pdf	1606014 2ce01a101c40f94b7b8a7c81f68508083e548737	no	2
Warnings:					
Information:					
45	Non Patent Literature	D1320.pdf	1689282 b7798cf17288dc3acb9307706c2a2a70973f184c	no	3
Warnings:					
Information:					
46	Non Patent Literature	D1321.pdf	1910327 e76ea173ade25cb899279ee9a0b4afe126acedd7	no	3
Warnings:					
Information:					
47	Non Patent Literature	D1322.pdf	1626309 514ab682b932d58d61a827a2118ddf49698bba89	no	5
Warnings:					
Information:					
48	Non Patent Literature	D1323.pdf	1422687 5053f6e89628e87a76c4cad00df2c78c6a197e8f	no	3
Warnings:					
Information:					
49	Non Patent Literature	D1324.pdf	1657880 35edfc131d77ab0ec4d915dba45b1baf8618fb7e	no	3
Warnings:					
Information:					
50	Non Patent Literature	D1325.pdf	1652566 4aac9ad54146c0b212453a0fb40c030213115806	no	2
Warnings:					
Information:					
51	Non Patent Literature	D1326.pdf	1606446 43858fe22b54c055fa9910bc4048b656fd73cefd	no	2
Warnings:					

Information:					
52	Non Patent Literature	D1327.pdf	1628105 79d0de0afe3ba9df8d2e319e29b95bf6e3b2438b	no	2
Warnings:					
Information:					
53	Non Patent Literature	D1328.pdf	1660574 a66b2834af80d0b20b1232eae9c600c8c01b3da8	no	3
Warnings:					
Information:					
54	Non Patent Literature	D1329.pdf	165761 2799ce86b9fb02f2610fd05e68b5c10d57929e46	no	3
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
55	Non Patent Literature	D1330.pdf	1528953 90841abd2aec80fd7db54dc354ba7471f1a537df	no	1
Warnings:					
Information:					
56	Non Patent Literature	D1331.pdf	1881993 525fd869875fc8b21e23fe137d6f9f10d443526b	no	4
Warnings:					
Information:					
57	Non Patent Literature	D1332.pdf	4208513 628abf59dd7c687a820cea0cc1221333b6da55f7	no	49
Warnings:					
Information:					
58	Non Patent Literature	D1333.pdf	406018 4584648447e1e1237ae7fe7a46a8811819c1b9d3	no	8
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
59	Non Patent Literature	D1334.pdf	468353 9a349f542457463d4bdf25df4272f7f2908469e3	no	11
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
60	Non Patent Literature	D1335.pdf	349555 d55c2ab36ca8783e35116e1d6333fdcfda5f181f	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
Total Files Size (in bytes):			162416634		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Electronic Acknowledgement Receipt

EFS ID:	15102745
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	04-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	11:53:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1367part77.pdf	5080937 c9aeb857311e82f677054681a14dc773defd5d3b	no	200

Warnings:

Information:

2	Non Patent Literature	D1367part78.pdf	5274671 708cbdfc075dbd09ceaf5511b91b095fdd6e9965	no	200
Warnings:					
Information:					
3	Non Patent Literature	D1367part79.pdf	6569921 1da47975c80f84d11cd8d8b097d5a432497bc43f	no	200
Warnings:					
Information:					
4	Non Patent Literature	D1367part80.pdf	6689283 045a83d2772c7dd35809ceecb9ba8b3d2f91c07f	no	200
Warnings:					
Information:					
5	Non Patent Literature	D1367part81.pdf	5447539 1f3b5c89c31c23e3c21668dccb615fe9fe5ab0c0	no	200
Warnings:					
Information:					
6	Non Patent Literature	D1367part82.pdf	5454275 42f253321fcb946f15f6b06c94adcc3cb6260af1	no	200
Warnings:					
Information:					
7	Non Patent Literature	D1367part83.pdf	5512481 49daf8c3370f73515395920b6aff5af913c7917e	no	200
Warnings:					
Information:					
8	Non Patent Literature	D1367part84.pdf	5319561 8b24b3553d256da42e4b44cb07b2366141720aad	no	200
Warnings:					
Information:					
9	Non Patent Literature	D1367part85.pdf	5516946 05541fe9c7bafcf80862e078892d159b7188cacb	no	200
Warnings:					
Information:					
10	Non Patent Literature	D1367part86.pdf	5082603 78d8c0955c95352592123011 9d98416974793bf6	no	200
Warnings:					
Information:					

11	Non Patent Literature	D1367part87.pdf	6006794 f2197a942a8d43c4923a1b839421fc2fa7c4fbe4	no	200
Warnings:					
Information:					
12	Non Patent Literature	D1367part88.pdf	5043145 fa379b985035db02f7bf256f674829d66ea9c0a7	no	200
Warnings:					
Information:					
13	Non Patent Literature	D1367part89.pdf	6423612 aa882a989be9579974a5b9e930d874de4c85d17e	no	200
Warnings:					
Information:					
14	Non Patent Literature	D1367part90.pdf	5293567 ce4708b0fab68d47c692cf45db1c80f7767377c8	no	200
Warnings:					
Information:					
15	Non Patent Literature	D1367part91.pdf	5481870 87c4160aed537a8949c8405ca44adcaf0cc1fc69	no	200
Warnings:					
Information:					
16	Non Patent Literature	D1367part92.pdf	6369650 5606b56694b6e467a3124540b457b504f73ca9cf	no	200
Warnings:					
Information:					
17	Non Patent Literature	D1367part93.pdf	5909805 fe992b1450fea1da6b9dfa7207a3528a79e68983	no	200
Warnings:					
Information:					
18	Non Patent Literature	D1367part94.pdf	5218581 55e986f3265c15475039bc763c44b88b81d91281	no	200
Warnings:					
Information:					
19	Non Patent Literature	D1367part95.pdf	5309204 43d2e3ac0ea579c1e86eb02fa5e21748511fe7b5	no	200
Warnings:					
Information:					

20	Non Patent Literature	D1367part96.pdf	4692277 98aa51f250cec36e9855e6e23a70889dc343 4578	no	200
Warnings:					
Information:					
21	Non Patent Literature	D1367part97.pdf	7427881 1fed39d36144aff06cce17da34dadce3fd01 5685	no	200
Warnings:					
Information:					
22	Non Patent Literature	D1367part98.pdf	7415097 cf79f150ec86fd6f0d38862fbf8e9a40ceb23 2cc	no	200
Warnings:					
Information:					
23	Non Patent Literature	D1367part99.pdf	4328217 17f6384afc549ac0a878e8b75430c58f7f3cd 37d	no	200
Warnings:					
Information:					
24	Non Patent Literature	D1367part100.pdf	4450138 c0d855ae089541f5881c67a6324f490fbb24 80c9	no	199
Warnings:					
Information:					
25	Non Patent Literature	D1367part101.pdf	7633741 dc3e7dbd30eea1d827f50181fd92e720a12 43a52	no	200
Warnings:					
Information:					
26	Non Patent Literature	D1367part102.pdf	6239272 f8fcd4c1fca498541612e72df5cd95020d36c 422	no	200
Warnings:					
Information:					
27	Non Patent Literature	D1367part103.pdf	6118485 d537b6bb3743838d991f3fa71a06999990b 02295	no	200
Warnings:					
Information:					
28	Non Patent Literature	D1367part104.pdf	6305558 bc39907953cc9bfa6be1c76a38c58074f412 9727	no	200
Warnings:					
Information:					

29	Non Patent Literature	D1367part105.pdf	6786238 d4ec58e22c6607f6a4435c4672b798af7022f505	no	200
Warnings:					
Information:					
30	Non Patent Literature	D1367part106.pdf	1857024 9759b7200ae7107d5e26c04d5a98eefb259da112	no	52
Warnings:					
Information:					
31	Non Patent Literature	D1367part107.pdf	2964766 ae5a72326e21c1fbe1ac9135c673f0e53493700b	no	198
Warnings:					
Information:					
32	Non Patent Literature	D1368.pdf	4010571 66eda3aa87b351f7a3dcf665f7a5bb668bcf6b56	no	18
Warnings:					
Information:					
33	Non Patent Literature	D1369.pdf	2056403 b2a95f7d98d3f163cb905c472f12762148e96fa8	no	8
Warnings:					
Information:					
34	Non Patent Literature	D1370.pdf	2578314 e2cf986767b9aa357b16bab04ab84b7900f5ba01	no	14
Warnings:					
Information:					
35	Non Patent Literature	D1371.pdf	2505462 7bb5878fb0e7ec7d03176d54f5b8f18e07c30e26	no	13
Warnings:					
Information:					
36	Non Patent Literature	D1372.pdf	1853041 757e5268612a855ffbefbecbe0e552195f952390	no	4
Warnings:					
Information:					
37	Non Patent Literature	D1373.pdf	2537596 dc0ad5cf25dbb7187b146f0cc63ca4fb5f2fb06f	no	8
Warnings:					
Information:					

38	Non Patent Literature	D1374.pdf	1977415 1ce1f630928a50231badb85c908b788d6755966a	no	4
Warnings:					
Information:					
39	Non Patent Literature	D1375.pdf	3710663 917cb9a7b3bdfea3ef674d221533f4bda978fb3d	no	27
Warnings:					
Information:					
40	Non Patent Literature	D1376.pdf	143571 fad0e8e3f3b9c45b319d5abae8e2ae4121d989ec	no	2
Warnings:					
Information:					
41	Non Patent Literature	D1377.pdf	169639 49df2a0869659c98b13aa37fb5cf678872bd1b75	no	19
Warnings:					
Information:					
42	Non Patent Literature	D1378.pdf	64023 41ca085d82ea2b7696453c8044626b59802a23d1	no	6
Warnings:					
Information:					
43	Non Patent Literature	D1379.pdf	777157 afe6e775d93ba3d86e5a5bff0fd6f203f7b41fa5	no	5
Warnings:					
Information:					
44	Non Patent Literature	D1380.PDF	455413 84c6b77cffcfdbac223b73c212ad01125d302b7c	no	4
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
45	Non Patent Literature	D1381.pdf	947802 e4c05ef39b7f2c97c1038700d9c76fd63685e643	no	12
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

46	Non Patent Literature	D1382.pdf	2879826 852d1ee843e763cf137a677fe9ff7278a599b3e3	no	49

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

47	Non Patent Literature	D1383.pdf	874110 900b29992eaff203bd50a0c2fbdb21e18eba0ef2	no	12

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

48	Non Patent Literature	D1384.pdf	1110254 d2b4480d886a6f366fdb29a4e402361d1d266502	no	19

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

49	Non Patent Literature	D1385.pdf	1724108 69f2e40fd553d3f12b73047669f74a9fd6ffff88	no	14

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

50	Non Patent Literature	D1386.pdf	1633320 53ba558f628dac2dc79f462c8be97a54d2664e5b	no	16

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

51	Non Patent Literature	D1387.pdf	2282409 c64b1394f297fa587fd3ca86e17112196f1c9d80	no	17

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

52	Non Patent Literature	D1388.pdf	973157 1b0d61a568425e353a519d0f574b890e60065bf0	no	11

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

53	Non Patent Literature	D1389.pdf	6081367 b3936e9347320ec1bad5a35984ea526a694d3105	no	59

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

54	Non Patent Literature	D1390.pdf	338445 4775ba71f03835afcde2e816a6a711ac0720fe0b	no	4

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

55	Non Patent Literature	D1391.pdf	292503 a6da97593470d7a9bfdc498737d336cb11894a88	no	3

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

56	Non Patent Literature	D1392.pdf	1035769 df0f983151570c455f870c2d09726f3c56f02b11	no	8

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

57	Non Patent Literature	D1393.pdf	9736160 690ab3b8b45484a583e03e513fd8dfabf58fbc25	no	83

Warnings:

Information:

58	Non Patent Literature	D1394.pdf	97596 970ea389448b4dc0ae7efc8562e425f182c86889	no	3

Warnings:

Information:

59	Non Patent Literature	D1395.pdf	337068 f616b207e367d403339d7bce73e919925887ccca	no	2

Warnings:

Information:					
60	Non Patent Literature	D1396.pdf	658944 441e7c81e2ca02615462fd3c26a0159a01feec75	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	227065245		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A163	5,007,051	04/09/1991	Dolkas et al.	
	A164	5,345,439	09/06/1994	Marston	
	A165	5,884,038	03/16/1999	Kapoor	
	A166	6,266,699	07/24/2001	Sevcik	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	C25	JP 09-270803	10/14/1997	Furukawa Electric Co. Ltd.		English Abstract	
	C26	JP 10-111848	04/28/1998	AT&T Corp.		English Abstract	
	C27	JP 10-215244	08/11/1998	Sony Corp.		English Abstract	
	C28	JP 04-117826	04/17/1992	Matsushita Electric Ind. Co. 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.	
	D1254	Eastlake, "Domain Name System Security Extensions," Network Working Group, RFC: 2535 pages 2-11 (March 1999)	
	D1255	Press Release; VirnetX and Aastra Sign a Patent License Agreement, 4 pages, May 2012, Printed from Website: http://virnetx.com/virnetx-and-aastra-sign-a-patent-license-agreement/	
	D1256	Press Release; VirnetX and Mitel Networks Corporation Sign a Patent License Agreement, 5 pages, July 2012, Printed from Website: http://virnetx.com/virnetx-and-mitel-networks-corporation-sign-a-patent-license-agreement/	
	D1257	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/vimetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1258	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001789 pp. 1-18, dated December 20, 2012	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1259	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001851 pp. 1-13, dated December 30, 2012	
	D1260	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001788 pp. 1-18, dated December 18, 2012	
	D1261	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001856 pp. 1-13, dated December 30, 2012	
	D1262	VirnetX vs Apple Transcript of Trial, Afternoon Session, 12:05 p.m., dated November 5, 2012	
	D1263	Certified Copy dated September 18, 2012 of U.S. Patent Number 6,502,135, 73 pages	
	D1264	Certified Copy dated December 30, 2009 of Assignment for Patent Application Number 95/047,83 12 pages	
	D1265	Certified Copy dated March 11, 2008 of Patent Application Number 09/504,783, 1500 pages	
	D1266	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,418,504, 74 pages	
	D1267	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number: 10/714,849, 10 pages	
	D1268	Certified Copy dated April 4, 2011 of Patent Application Number 10/714,849, 1170 pages	
	D1269	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,490,151, 63 pages	
	D1270	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number 10/259,494, 19 pages	
	D1271	Certified Copy dated April 4, 2011 of Application Number 10/259,454, 1359 pages	
	D1272	Certified Copy dated April 12, 2011 of U.S. Patent Number 7,921,211, 78 pages	
	D1273	Certified Copy dated October 17, 2012 of Assignment for Application Number 11/840,560, 12 pages	
	D1274	Certified Copy dated April 20, 2011 of Application Number 11/840,560, 3 pages	
	D1275	iPhone User Guide for iPhone OS 3.1 Software, 217 pages, 2009	
	D1276	iPhone User Guide for iOS 4.2 and 4.3 Software, 274 pages, 2011	
	D1277	iPhone User Guide for iPhone and iPhone 3G, 154 pages, 2008	
	D1278	iPhone User Guide for iOS 5.0 Software, 163 pages, 2011	
	D1279	iPad User Guide for iOS 5.0 Software, 141 pages, 2011	
	D1280	iPad User Guide for iOS 4.2 Software, 181 pages, 2010	
	D1281	iPad User Guide for iOS 4.3 Software, 198 pages, 2011	
	D1282	iPad User Guide, 154 pages, 2010	
	D1283	iPod Touch User Guide for iOS 5.0 Software, 143 pages, 2011	
	D1284	iPod Touch User Guide, 122 pages, 2008	
	D1285	iPod Touch User Guide for iPhone OS 3.0 Software, 153 pages, 2009	
	D1286	iPod Touch User Guide for iPhone OS 3.1 Software, 169 pages, 2009	
	D1287	iPod Touch User Guide for iOS 4.3 Software, 230 pages, 2011	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1288	iPod Touch Features Guide, 98 pages, 2008	
	D1289	VPN Server Configuration for iOS; Networking & Internet Enterprise Deployment, 12 pages, 2011	
	D1290	iPhone Configuration Utility User Guide, 26 pages, 2010	
	D1291	iPhone Configuration Utility; Networking & Internet: Enterprise Deployment, 26 pages, 2011	
	D1292	iPhone Configuration Utility; Networking>Internet & Web, 24 pages, 2010	
	D1293	iOS Configuration Profile Reference; Networking & Internet: Enterprise Deployment, 24 pages, 2011	
	D1294	iPhone OS Enterprise Deployment Guide; Second Edition, for Version 3.1 or Later, 91 pages, 2009	
	D1295	iPhone OS; Enterprise Deployment Guide; Second Edition, for Version 3.2 or Later, 90 pages, 2010	
	D1296	CFHost Reference; Developer, 20 pages, 2008	
	D1297	CFNetwork Programming Guide; Developer, 60 pages, 2011	
	D1298	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1299	Mac OS X Devloper Library; CFHostSample.c, 1 page	
	D1300	Mac OS X Developer Library; CFHostSample, 1 page, 2004	
	D1301	Mac OS X Developer Library; Document Revision History, 1 page, 2004	
	D1302	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1303	Apple Push Notification Service; Distribution Service, Version 1.0, 6 pages, 2009	
	D1304	iOS Human Interface Guidelines; Developer, 184 pages, 2012	
	D1305	Networking & Internet Starting Point, 3 pages, 2011	
	D1306	Server Admin. 10.5 Help; Viewing a VPN Overview, 1 page	
	D1307	iOS: Supported Protocols for VPN, 2 pages, 2010	
	D1308	IPhone in Business Virtual Private Networks (VPN), 3 pages, 2010	
	D1309	iPhone and iPad in Business Deployment Scenarios, 26 pages, 2011	
	D1310	Deploying iPhone and iPad Virtual Private Networks, 3 pages, 2011	
	D1311	Deploying iPhone and iPad; Security Overview, 6 pages, 2011	
	D1312	Pad in Business; "Ready for Work," 2012, 5 pages	
	D1313	iOS: Using FaceTime, 2 pages, 2011, Printed from website http://support.apple.com/kb/HT4317	
	D1314	MobileMe: "Secure Chat" is Unavailable in OS X Lion, 2 pages, 2012, Printed from Website: http://support.apple.com/kb/TS3902	
	D1315	iPhone 4 and iPod Touch (4th Generation): Using FaceTime, 2 pages, 2010, Printed from Website: http://support.apple.com/kb/HT4319	
	D1316	IPhone; "Picking Up Where Amazing Left Off," 11 pages, 2012, Printed from Website: http://www.apple.com/iPhone/features/facetime	
	D1317	FaceTime for Mac; "Say Hello to FaceTime for Mac," 4 pages, 2012, Printed from Website: http://www.apple.com/mac/facetime	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1318	iPad; "Your New Favorite Way to do Just About Everything," 8 pages, 2012, Printed from Website" http://www.apple.com/ipad/built-in-apps/	
	D1319	iPod Touch; FaceTime, "Oh, I see what you're saying," 2 pages	
	D1320	Apple Press Info; Apple Presents iPhone 4, Printed from Website: http://www.apple.com/pr/library/apple-presents-iphone	
	D1321	iPod Touch; FaceTime, "Oh I See What You're Saying,", 3 pages, 2012, Printed from Website: http://www.apple.com/iPodtouch/built-in-apps/facetime.htm	
	D1322	IOS 4, The World's Most Advanced Mobile Operating System, 5 pages, Printed from Website: http://www.apple.com/iphone/ios4	
	D1323	Apple Press Info; Apple Reinvents the Phone with iPhone, 3 pages, 2007, Printed from Website: http://www.apple.com/pr/library/2007/01/09Apple-reinvents-the-phone	
	D1324	Apple Press Info; Apple Announces the New iPhone 3Gs-The Fastest, Most Powerful iPhone Yet, 3 pages, 2009, Printed from the Website: http://www.apple.com/pr/library/2009/06/08Apple-Announces-the-new-iphone3GS	
	D1325	Apple Press Info; Apple Launches iPhone 4S, ios 5 & iCloud, iPhone 4S Features Dual-Core A5 Chip, All New Camera, full 1080p HD Video Recording & Introduces Siri, 2011, 2 pages, Printed from website: http://www.apple.com/pr/library/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud.html	
	D1326	Apple Press Info; Apple Introduces New iPod Touch, Features Retina Display, A4 Chip, FaceTime Video Calling, HD Video Recording & Game Center, 2 pages, 2010, Printed from Website http://www.apple.com/pr/library/2010/09/01Apple-Introduces-New-iPod-touch.html	
	D1327	Apple Press Info; Apple Launches iPad, Magical & Revolutionary Device at an Unbelievable Price, 2 pages, 2010, Printed from Website: http://www.apple.com/pr/library/2010/01/27Apple-Launches-iPad.html	
	D1328	Apple Press Info; Apple Launces New iPad, New iPad Features Retina Display, A5X Chip, 5 Megapixel iSight Camera & Ultrafast 4G LTE, 2012, 3 pages, Printed from the Website: http://www.apple.com/pr/library/2012/03/07Apple-Launches-New-iPad.html	
	D1329	FaceTime; "Phone Calls Like You've Never Seen Before," 3 pages	
	D1330	Apple Press Info; Apple Brings FaceTime to the Mac, 1 pages, Printed from Website https://www.apple.com/pr/library/2010/10/20Apple-Brings-FaceTime-to-the-Mac.html	
	D1331	iPad at Work; "Mobile Meetings Made Easy," 4 pages, 2011	
	D1332	IPad – Technical Specifications, 49 pages, Printed from Website: http://support.apple.com/kb/sp58C	
	D1333	Stirling Design, 8 pages, 2008	
	D1334	Quick Guide: SSL VPN Technical Primer, 11 pages, 2010	
	D1335	Silva, "Secure iPhone Access to Corporate Web Applications," Technical Brief, 10 pages	
	D1336	Defendant Apple Inc.'s Third Supplemental Responses to VirnetX Inc.'s First Request for Admission to Apple Inc. dated, April 13, 2012, 207 pages	
	D1337	Apple Support Communities, 4 pages, Printed from Website https://discussions.apple.com/thread/486096?start=0&tstart=0	
	D1338	VirnetX – Products; License and Service Offerings, 1 page	
	D1339	VirnetX Contact Information, 4 pages, 2011	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1340	VirnetX Launches Secure Domain Name Initiative; 4G/LTE Security, 1 page, 2010	
	D1341	VirnetX Gabriel Connection; Enabling Safe Network Neighborhoods, 2 pages, 2012	
	D1342	Baugher et al., "The Secure Real-Time Transport Protocol (SRTP)," Network Working Group, RFC:3711, 39 pages, 2004	
	D1343	Jennings et al., "Resource Location and Discovery (Reload) Draft-Bryan-P2PSIP-Reload-04," Internet-Draft, 12/12/08, pages 1-127	
	D1344	Barnes et al., "Verification Involving PSTN Reachability: Requirements and Architecture Overview," Internet Draft, 27 pages, 2012	
	D1345	April Inc. Form 10-K (Annual Report) filed 12/01/05 for the Period Ending 09/24/05, Edgar Online, 1400 pages, 2011	
	D1346	Phone, Facetime; "Be in Two Places at Once," 3 pages, Printed from the Website http://www.apple.com/ios/facetime/	
	D1347	Apple Press Info; Apple Presents iPhone 4, All-New Design with FaceTime Video Calling, Retina, Display, 5 Megapixel Camera & HD Video Recording, 3 pages, 2010	
	D1348	NYSE AMEX:VHC; Cowen and Co. 39th Annual Technology Media & Telecom Conference, 36 pages, June 2, 2011	
	D1349	Pindyck et al., "Market Power: Monopoly and Monopsony," Microeconomics, Sixth Edition, pages 370-371	
	D1350	Press Release; IpCapital Group Completes VirnetX IP Licensing Evaluation, 3 pages	
	D1351	Microsoft Real-Time Communications: Protocols and Technologies, Microsoft TechNet, 22 pages, 2010	
	D1352	Filing Receipt dated September 23, 2011 for Application Number: 13/223,259	
	D1353	Email Communications Regarding Apple Product Innovations, 6 pages, 2010	
	D1354	Mathy et al., "Traversal Using Relays Around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," Internet Engineering Task Force (IETF), RFC: 5766, 67 pages, 2010	
	D1355	Egevang et al., "The IP Network Address Translator (NAT)," Network Working Group, RFC: 1631, 10 pages, 1994	
	D1356	Srisuresh et al., "IP Network Address Translator (NAT) Terminology and Considerations," Network Working Group, RFC:2663, 30 pages, 1999	
	D1357	Sisalem, et al., "Introduction to Cryptographic Mechanisms," SIP Security, 356 pages, 2009	
	D1358	Curriculum Vitae, Mark T Jones, 9 pages	
	D1359	Curriculum Vitae, Roy Weinstein, 5 pages	
	D1360	How To Configure IPSec Tunneling in Windows 2000, 8 pages	
	D1361	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/vimetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1362	iPhone, FaceTime; "Be in Two Places at Once," 3 pages, Printed from Website: http://www.apple.com/ios/facetime/	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1363	iPhone, "It Does Everything Better,"6 pages, Printed from Website: http://www.apple.com/iPhone/built-in-apps	
	D1364	My Apple ID, "What's an Apple ID," 1 pages, Printed from Website: https://appleid.apple.com/cgi-bin/webobjects/myappleid.woa	
	D1365	Rosenberg et al., "Session Initiation Protocol (SIP): Locating SIP Servers," Network Working Group, RFC: 3263, 17 pages, 2002	
	D1366	Certified Copy dated September 21, 2012 of Reexamination Certificate Number 6,502,135 issued June 6, 2011, 11 pages	
	D1367	Certified Copy dated September 20, 2012 of Patent Application Number 95/001,269	
	D1368	Chatterjee et al., "Bargaining Under Incomplete Information," Operations Research, 31:835-851, 1983	
	D1369	Nash, "The Bargaining Problem," Econometrica, 18:155-162, 1950	
	D1370	Nash, "Two-Person Cooperative Games," Econometrica, 21:128-140, 1953	
	D1371	Choi et al., "An Analytical Solution to Reasonable Royalty Rate Calculations," IDEA: The Journal of Law and Technology, 13 pages, 2001	
	D1372	The Prize in Economics 1994 - Press Release dated October 11, 1994, 4 pages, Printed from Website: http://www.nobelprize.org/nobel_prizes/economics/laureates/1994/press.html	
	D1373	Putnam et al., "Bargaining and the Construction of Economically Consistent Hypothetical License Negotiations," The Licensing Journal, pages 8-15, 2004	
	D1374	Scherling et al., "Rational Reasonable Royalty Damages: A Return to the Roots," Landslide, Volume 4, 4 pages, 2011	
	D1375	Jarosz et al., "Application of Game Theory to Intellectual Property Royalty Negotiations," Chapter 17, pages 241-265	
	D1376	Goldscheider, Licensing Best Practices; Strategic, Territorial, and Technology Issues, 2 pages, 2006	
	D1377	iPhone Configuration Utility, 19 pages, 2012	
	D1378	VPN Server Configuration for iOS Devices, 6 pages, 2012	
	D1379	Samuelson et al., Economics, Fourteenth Edition, pages 258-259, 1992	
	D1380	Stigler et al., The Theory of Price, Forth Edition, pages 215-216, 1987	
	D1381	Truett et al., "Joint Profit Maximization, Negotiation, and the Determinacy of Price in Bilateral Monopoly," Journal of Economic Education, pages 260-270	
	D1382	Binmore et al., "Noncooperative Models of Bargaining," The Handbook of Game Theory, 1:(7)181-225,1992	
	D1383	Spindler et al., "Endogenous Bargaining Power in Bilateral Monopoly and Bilateral Exchange," Canadian Journal of Economics-Revue Canadienne D Economie, pages 464-474, 1974	
	D1384	Myerson, "Game Theory; Analysis or Conflict," Harvard University Press, pages 375-392	
	D1385	Binmore, "The Nash Bargaining Solution in Economic Modelling," The Rand Journal of Economics, 17:176-188, 1996	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1386	Rubinstein et al., "On the Interpretation of the Nash Bargaining Solution and its Extension to Non-Expected Utility Preferences," Econometrica, 60:1171-1186, 1992	
	D1387	Greenleaf et al., "Guarantees in Auctions: The Auction House as Negotiator and Managerial Decision Maker," Management Science, 39:1130-1145, 1993	
	D1388	Chan, "Trade Negotiations in a Nash Bargaining Model," Journal of International Economics, 25:253-363, 1987	
	D1389	Lemley et al., "Patent Holdup and Royalty Stacking," Texas Law Review, 85:1991-2049	
	D1390	Cauley, "Winning the Patent Damages Case; A Litigator's Guide to Economic Models and Other Damage Strategies," Oxford Press, pages 29-30, 2044	
	D1391	Degnan et al., "A Survey of Licensed Royalties," Les Nouvelles, pages 91, 93, 94, 1997	
	D1392	Kahn, "The Review of Economics and Statistics," pages 157-164, 1993	
	D1393	Microsoft Company Information; Including Stocks and Financial Information, 83 pages	
	D1394	Apple Press Info: Apple Updates MacBook Pro with Next Generation Processors, Graphics & Thunderbolt I/O Technology, 3 pages, Printed from Website: http://www.apple.com/pr/library/2011/02/24Apple-Updates-MacBook-Pro-with-Next-Generation-Processors-Graphics-Thunderbolt-I-O-Technology.html	
	D1395	Apple Press Info: Apple to Ship Mac OS X Snow Leopard on August 28, 2 pages, Printed from the Website: http://www.apple.com/pr/library/2009/08/24/apple-to-ship-mac-os-x	
	D1396	iPad, Facetime; "Once Again, iPad gets the World Talking," 3 pages, Printed from the Website: http://www.apple.com/ipad/built-in-apps/facetime/html	
	D1397	Apple iOS: Setting up VPN, 2 pages, Printed from Website: http/support.apple.com/kb/HT1424	
	D1398	Apple iPhone User Guide for iOS 5.1 Software, 179 pages, 2012	
	D1399	Apple, Communicating with HTTP Servers, CFNetworking Programming Guide, 6 pages, 2011, Printed from the Website: https://developer.apple.com/library/ios/documentation/networking/conceptual/CFNetwork/CFHT	
	D1400	VirnetX, Gabriel Connection Technology ™ White Paper, 7 pages, 2012	
	D1401	VirnetX, Technology, 4 pages, 2012	
	D1402	Certified Copy dated January 15, 2008 of U.S. Patent Number 6,502,135, 64 pages	
	D1403	Inter Partes Reexamination Certificate dated June 7, 2011 for Patent Number 6,502,135	
	D1404	Proceedings of The Symposium on Network and Distributed System Security, 7 pages, February 22-23, 1996	
	D1405	In-Q-Tel; Corporate Overview, 2 pages, 2004	
	D1406	Davies, Supervisor of Translation: Tadahiro Uezono, Security for Computer Networks, Japan, Nikkei-McGraw-Hill Inc., First Edition, First Copy, p 126-129 (December 5, 1985) – (English Version and Japanese Version Submitted)	
	D1407	Comer, "Translated by Jun Murai and Hiroyuki Kusumoto, "Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture, Third Edition," Japan Kyoritsu Shuppan Co., Ltd., First Edition, First Copy, p 161-193 (August 10, 1997) (English Version and Japanese Version Submitted)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1408	Lynch et al., Supervisor of Translation: Jun Murai, "Internet System Handbook," Japan Impress Co. Ltd. First Edition p 152-157 and p 345-351 (August 11, 1996) (English Version and Japanese Version Submitted)	
	D1409	Office Action dated December 27, 2012 from Corresponding Canadian Patent Application Number 2723504	
	D1410	Office Action dated December 5, 2012 from Corresponding Japanese Patent Application Number 2011-081417	
	D1411	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-085052	
	D1412	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-083415	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**13/339,257**
				Filing Date	**12-28-2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Krisna Lim**
				Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

This Information Disclosure Statement is being filed after the receipt of the final office action dated December 10, 2012.

The references contained in the Information Disclosure Statement were either; cited in a communication from a foreign patent office in a counterpart foreign application, and, to the was known to any individual designated in § 1.56(c) more than three months prior to the filing of the Information Disclosure Statement, or, received from the client no more than three months prior to the filing of this Information Disclosure Statement.

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[X] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or; Cited reference A163 from Canadian office action dated December 27, 2012; Cited reference C25 from Japanese office action dated 12/13/12; Cited references C26, D1254 from Japanese office action dated 12/13/12; C27-C28, D1406-1408 from Japanese office action dated 12/05/12.

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement. Cited references A164-A166 cited by examiner in office action dated December 5, 2012 for U.S. patent application number: 13/617,375; D1255-D1405 all received by the client on January 31, 2013.

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $930.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

/Toby H. Kusmer/

Date: March 1, 2013

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

DM_US 41379925-1.077580.0154

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-270803**

(43)Date of publication of application : **14.10.1997**

---

(51)Int.Cl. **H04L 12/28**

H04L 12/46

H04L 12/66

H04Q 3/00

---

(21)Application number : **08-080005**

(22)Date of filing : **02.04.1996**

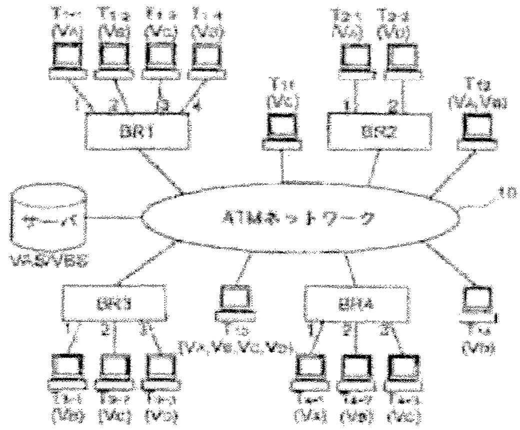
(71)Applicant : **FURUKAWA ELECTRIC CO LTD:THE**

(72)Inventor : **HORIGUCHI MASANORI**
SUZUKI ATSUHIKO

---

(54) **VIRTUAL NETWORK CONSTITUTING METHOD**

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the load of group management in a bridge or an asynchronous transfer mode(ATM) terminal equipment belonging to plural groups.
SOLUTION: In this method, bridges BR1-BR4 each connecting to LAN terminal equipments and ATM terminal equipments T11-T14 are connected directly to an ATM network 10, the terminal equipments are grouped and a VLAN is set to the groups, and data communication is conducted between a sender terminal equipment and a terminal equipment whose communication is allowed. In this case, address information and group identification information of the bridges and the ATM terminal equipments are registered in cross reference with each other in a 1st address table in a server VAS/VBS, and with respect to an inquiry of an ATM address of a destination conducted prior to data communication, the server retrieves the 1st address table and returns an acknowledge frame to an equipment making the inquiry, so that the data communication is conducted only between terminal equipments whose communication is allowed.



CLAIMS

[Claim(s)]
[Claim 1]While carrying out direct continuation of repeating installation which has two or more ports where the 1st terminal unit is connected, respectively, and a bridge function, and the 2nd terminal unit via a trunk network, In a system which performs data communications between the aforementioned terminal units by which carried out the group division of each port and the 2nd terminal unit of the aforementioned repeating installation, and set up a virtual network, and the communication permission was carried out to a transmission source terminal,
As opposed to an inquiry of a network address of an address characterized by comprising the following which makes connect a memory response means to the aforementioned trunk network, and is performed in advance of the aforementioned data communications, A virtual network constructing method, wherein the aforementioned memory response means returns a predetermined response to equipment which performed the aforementioned inquiry so that data communications can be performed only between terminal units by which searched said 1st address storage section and the communication permission was carried out [aforementioned].
Address information of the aforementioned repeating installation and the 2nd terminal unit.
At least one group identification information to which this repeating installation and the 2nd terminal unit belong.
The 1st address storage section that makes bit information which shows that it is the repeating installation to which several 1st terminal units with which at least one differs in the aforementioned group who does a group are connected correspond, and memorizes it.

[Claim 2]The virtual network constructing method comprising according to claim 1:
Address information which the aforementioned trunk network consisted of ATM networks, and the aforementioned network address consisted of ATM addresses, and was memorized by said 1st address storage section is a MAC Address of the aforementioned repeating installation and the 2nd terminal unit.
An ATM address corresponding to this MAC Address.

[Claim 3]A group to whom equipment which the aforementioned memory response means searched group identification information corresponding to an address of equipment which performed the aforementioned inquiry from said 1st address storage section, and performed this inquiry belongs, The virtual network constructing method according to claim 1 returning the aforementioned predetermined response to equipment which performed this inquiry only when communication is permitted among groups to whom a destination device of this inquiry belongs.
[Claim 4]The virtual network constructing method according to claim 1 or 3 returning a predetermined response characterized by comprising the following to the

aforementioned memory response means.
To an inquiry of a network address of an address which is not memorized by said 1st address storage section, the aforementioned memory response means, A MAC Address of each 1st terminal unit that transmits this inquiry to the aforementioned repeating installation and the 2nd terminal unit other than equipment which performed this inquiry and by which the aforementioned repeating installation was connected to self-equipment.
Group identification information corresponding to [have the 2nd address storage section that makes group identification information to which this each 1st terminal unit belongs correspond, and memorizes it, search the 2nd address storage section to an inquiry of an address of this 1st terminal unit, and] a corresponding address.

[Claim 5]A network address of an address where repeating installation which performed the aforementioned inquiry was obtained by the predetermined response from the aforementioned memory response means, As opposed to an address of a transmission frame from the 1st terminal unit that has the 3rd address storage section that corresponds and memorizes group identification information to which this address belongs, and was connected to self-equipment, The virtual network constructing method according to claim 1 or 3 characterized by sending out this transmission frame to the aforementioned trunk network only when communication is permitted between a group who searches this 3rd address storage section, and to whom an address belongs, and a group to whom the 1st terminal unit concerned belongs.
[Claim 6]When a frame which should be carried out the multiple address is received, the aforementioned memory response means from a group identification descriptor added to search results or this multiple address frame of said 1st address storage section, The virtual network constructing method according to claim 1, 3, or 4 transmitting this multiple address frame to a group's repeating installation or 2nd terminal unit to which it was added by the address concerned only when communication is permitted among groups to whom a group to whom a transmitting agency belongs is judged and this transmitting origin belongs.
[Claim 7]The aforementioned memory response means searches said 1st address storage section, when transmitting the aforementioned multiple address frame, The virtual network constructing method according to claim 4 or 6 adding group identification information of a transmitting agency to this multiple address frame, and transmitting it when the destination of this multiple address frame is the repeating installation to which several 1st terminal units with which at least one differs in the aforementioned group who does a group are connected.
[Claim 8]As opposed to a multiple address frame from the 1st terminal unit by which the aforementioned repeating installation was connected to self-equipment, Search said 2nd address storage section and a multiple address frame which added group identification information to which this 1st terminal unit belongs is sent out to the aforementioned memory response means, A multiple address frame transmitted from this memory response means is received, The virtual network constructing method according to claim 4, 6, or 7 relaying this multiple address frame only to the 1st terminal unit that searches said 2nd address storage section and belongs to this group based on group identification information added to this multiple address frame.
[Claim 9]While carrying out direct continuation of repeating installation which has two or more ports where the 1st terminal unit is connected, respectively, and a bridge function, and the 2nd terminal unit via a trunk network, In a system which performs data communications between terminal units by which carried out the group division of each port and the 2nd terminal unit of the aforementioned repeating installation, and set up a virtual network, and the communication permission was carried out to a transmission source terminal,
Make it connect with the aforementioned trunk network, and a multiple address means

characterized by comprising the following the aforementioned multiple address means, When a frame which should be carried out the multiple address is received, from a group identification descriptor added to search results or this multiple address frame of said 1st address storage section, A virtual network constructing method transmitting this multiple address frame to a group's repeating installation or 2nd terminal unit to which it was added by the address concerned only when communication is permitted among groups to whom a group to whom a transmitting agency belongs is judged and this transmitting origin belongs.
Address information of the aforementioned repeating installation and the 2nd terminal unit.
At least one group identification information to which this repeating installation and the 2nd terminal unit belong.
The 1st address storage section that makes bit information which shows that it is the repeating installation to which several 1st terminal units with which at least one differs in the aforementioned group who does a group are connected correspond, and memorizes it.

[Claim 10]The virtual network constructing method comprising according to claim 9:
Address information which the aforementioned trunk network consisted of ATM networks, and the aforementioned network address consisted of ATM addresses, and was memorized by said 1st address storage section is a MAC Address of the aforementioned repeating installation and the 2nd terminal unit.
An ATM address corresponding to this MAC Address.

[Claim 11]The aforementioned multiple address means searches said 1st address storage section, when transmitting the aforementioned multiple address frame, The virtual network constructing method according to claim 9 adding group identification information of a transmitting agency to this multiple address frame, and transmitting it when the destination of this multiple address frame is the repeating installation to which several 1st terminal units with which at least one differs in the aforementioned group who does a group are connected.
[Claim 12]A MAC Address of each 1st terminal unit by which the aforementioned repeating installation was connected to self-equipment, As opposed to a multiple address frame from the 1st terminal unit that has the 2nd address storage section that makes group identification information to which this each 1st terminal unit belongs correspond, and memorizes it, and was connected to self-equipment, Search said 2nd address storage section and a multiple address frame which added group identification information to which this 1st terminal unit belongs is sent out to the aforementioned memory response means, A multiple address frame transmitted from this memory response means is received, The virtual network constructing method according to claim 9 or 11 relaying this multiple address frame only to the 1st terminal unit that searches said 2nd address storage section and belongs to this group based on group identification information added to this multiple address frame.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]The present invention relates to the virtual network constructing method which builds the virtual LAN by which grouping was carried out virtually among two or more terminal units connected to trunk networks, such as an ATM (Asynchronous Transfer Mode) network, via repeating installation.
[0002]
[A related background art] Regardless of physical composition called wiring between

the position of the terminal unit in a network, or these terminal units, conventionally, The technology of building LAN in workgroup units, such as a brokerage department, development departments, and a research section, is known for "inrush, virtual LAN", etc. which were described, for example in the Nikkei communication No. (November 21, 1994 issue) 186. Since such LAN builds a network based on a logical group division, it is called virtual (virtual) LAN.

[0003]As a means to build the above-mentioned virtual LAN, there was the method of assigning a virtual LAN identifier (henceforth "VID") peculiar to a workgroup for every LAN port of a bridge using a bridge (it is also called switching HUB) with two or more LAN ports. However, the increase in the terminal unit connected was not able to be coped with by this method.

[0004]So, in the former, the LAN emulation standardized by ATM Forum is used, For example, the terminal unit which constitutes two or more LAN based on the standard of IEEE802.3 or IEEE802.5, It connected with the high-speed ATM network via the bridge, and there was the method of making the virtual LAN equivalent to the above-mentioned workgroup correspond to two or more ELAN(s) (emulated LAN) built on the above-mentioned ATM network, and applying to them. In this method, an address solution server and a multiple address server corresponding for every ELAN are provided, and the MAC Address (physical address) and ATM address of a terminal unit or a bridge which belong to applicable ELAN become a pair, and are registered into the address solution server.

[0005]In this method, when unicast communication was performed, previously, by asking an address solution server the ATM address of an address, the terminal unit had a connection to a destination device, and had enabled communication to a destination device. When multicast communication was performed, multicast transfer within a group was performed by transmitting the frame transmitted to the multiple address server from the transmitting agency to all the terminal units and bridge belonging to ELAN to which a multiple address server corresponds.

[0006]

[Problem to be solved by the invention]However, a terminal unit by which direct continuation was carried out to the ATM network in the described method. (It is hereafter called "ATM terminal equipment") Since the ELAN parameter managed in a bridge, for example, a local station address, the server address, the control-system timer counter, etc. became largely in proportion to group number, there was a problem that the load in respect of network management became largely.

[0007]In the network side, an address solution server and a multiple address server corresponding for every group had to be extended, and there was a problem that a manufacturing cost became high. With management of these servers, each terminal unit side also had to manage the connection (connection path of an ATM cell switch) which leans between servers for every group, and also had the problem that the load in respect of group management became largely.

[0008]If groups differ even if it is communication between the same ATM terminal equipment and a bridge physically, a different connection must be established each time using signaling processing. Therefore, when two or more communication paths existed between the same ATM terminal equipment and a bridge, the judging process to which path the frame of the terminals belonging to two or more groups transmitted had to be performed, and there was a problem that communications processing became complicated.

[0009]When two or more communication paths existed between the same ATM terminal equipment and a bridge in transmission of a multiple address frame, there was a problem that a frame might overlap and it might arrive by a receiving side. The present invention was made in view of the above-mentioned problem, and an object of the present invention is to provide the virtual network constructing method which can reduce the load of the group management in the bridge or ATM terminal equipment belonging to two or more groups.

[0010]There are other purposes of the present invention in performing establishment and band utilization of an efficient connection while making the minimum resources, such as an address solution server by the side of a network, and a multiple address server. Other purposes of the present invention are to provide the virtual network constructing method which can maintain interconnectivity with the existing terminal unit, without making special processing perform to the conventional terminal unit.

[0011]

[Means for solving problem]Repeating installation (bridge) which has two or more ports where the 1st terminal unit is connected, respectively, and a bridge function in the present invention in order to attain the above-mentioned purpose, While carrying out direct continuation of the 2nd terminal unit via a trunk network (ATM network), In the system which performs data communications between the terminal units by which carried out the group division of each port and the 2nd terminal unit of the aforementioned bridge, and set up the virtual network, and the communication permission was carried out to the transmission source terminal, The MAC Address of a bridge and the 2nd terminal unit, and the address information of an ATM address, At least one group identification information to which a bridge and the 2nd terminal unit belong, The memory response means which has the 1st address storage section (the 1st address table) that makes the bit information (flag) which shows that it is a bridge to which several 1st terminal units with which at least one differs in the aforementioned group who does a group are connected correspond, and memorizes it (the function of an address solution server and a multiple address server) Connect the server which it has to an ATM network, and a server searches the group identification information corresponding to the address of the equipment which asked from the 1st address table to the inquiry of the ATM address of an address performed in advance of data communications, Only when communication is permitted between the group to whom the equipment which asked belongs, and the group to whom the destination device of an inquiry belongs, a predetermined response is returned to the equipment which performed the aforementioned inquiry so that data communications can be performed between the terminal units by which the communication permission was carried out.

[0012]In Claim 4, to an inquiry of the ATM address of the address which is not memorized by the 1st address table, a server, To a bridge and the 2nd terminal unit other than the equipment which performed this inquiry, transmit this inquiry, and to them a bridge, Have the 2nd address table that makes the MAC Address of the 1st terminal unit connected to self-equipment, and the group identification information to which this each 1st terminal unit belongs correspond, and memorizes them, and an inquiry of the address of this 1st terminal unit is received, The 2nd address table is searched and the predetermined response include the group identification information corresponding to a corresponding address is returned to a server.

[0013]In Claim 5, the bridge which asked, As opposed to the address of the transmission frame from the 1st terminal unit that has the 3rd address table that corresponds and memorizes the ATM address of the address obtained by the predetermined response from a server, and the group identification information to which this address belongs, and was connected to self-equipment, The 3rd address table is searched, and only when communication is permitted between the group to whom an address belongs, and the group to whom the 1st terminal unit concerned belongs, a transmission frame is sent out to an ATM network.

[0014]When a server receives the frame which should be carried out the multiple address in Claim 6 and 9, From the group identification descriptor added to the search results or this multiple address frame of the 1st address table, The group to whom a transmitting agency belongs is judged, and only when communication is permitted among the groups to whom this transmitting origin belongs, this multiple address frame is transmitted to a group's bridge or 2nd terminal unit to which it was added by the

address concerned.
[0015]As opposed to the multiple address frame from the 1st terminal unit by which repeating installation was connected to self-equipment in Claim 8 and 12, Search the 2nd above-mentioned address table and the multiple address frame which added the group identification information to which this 1st terminal unit belongs is sent out to a server, To the multiple address frame transmitted from the server, based on the group identification information added to this multiple address frame, the 2nd above-mentioned address table is searched and this multiple address frame is relayed only to the 1st terminal unit belonging to this group.
[0016]
[Mode for carrying out the invention]The virtual network constructing method concerning the present invention is described based on the Drawings of Fig.1 thru/or Fig.5.Fig.1 is a configuration diagram showing the composition of one working example of the virtual LAN system using the virtual network management method concerning the present invention, It is one working example which built virtual LAN (henceforth "VLAN") using the LAN emulation (specification for using the existing LAN property in the ATM environment) of the ATM Forum conformity. It has on backbone a high-speed network like ATM network 10 which comprises an ATM cell switch which is not illustrated by a VLAN system in a figure, Direct continuation of two or more bridges BR1-BR4, ATM terminal equipment T11-T14, and server VAS/VBS is carried out to ATM network 10, and it is constituted.
[0017]The ATM network side port where the bridges BR1-BR4 are connected with ATM network 10, It has a branch line LAN side port where a terminal unit is connected, respectively, and bridging connection in the MAC layer level is performed between the ports of self-equipment between the ATM network side ports with other bridges and ATM terminal equipment. The bridges BR1-BR4 can also be set [to which VLAN each branch line LAN side port belongs independently by having a function of VLAN, and] up so that it can set up and one port may belong to two or more VLAN(s) in that case. Different VLAN is identified as different emu rhe TITTO LAN (ELAN) on ATM network 10. Thereby, it becomes possible to build VLAN ranging over the bridges BR1-BR4. In the function of this VLAN, a multicast packet (a broadcasting packet is also included) is not transmitted between different VLAN(s).
[0018]The bridges BR1-BR4 have accommodated branch line LAN belonging to two or more groups, In each branch line LAN side port 1-4 of bridge BR1, a terminal unit of each branch line LAN. (It is hereafter called "LAN terminal equipment") T1-1 - T1-4 in each branch line LAN side port 1 and 2 of bridge BR2 LAN-terminal-equipment T2-1 and T2-2, LAN-terminal-equipment T3-1 - T3-3 are connected to each branch line LAN side port 1-3 of bridge BR3, and LAN-terminal-equipment T4-1 - T4-3 are connected to each branch line LAN side port 1-3 of bridge BR4, respectively.
[0019]In this example, MAC Addresses T1-T4 and ATM address A1 - A4 are set to the bridges BR1-BR4, respectively. The MAC Address T1-1 - T1-4 [same] as the above-mentioned sign, T2-1, T2-2, T3-1 - T3-3, T4-1 - T4-3 are set as LAN-terminal-equipment T1-1 - T1-4, T2-1, T2-2, T3-1 - T3-3, T4-1 - T4-3, respectively. Direct continuation of the ATM terminal equipment T11-T14 is carried out to ATM network 10, and same MAC Addresses T11-T14 and ATM addresses A11-A14 as the above-mentioned sign are set up.
[0020]These terminal units belong to one which is identified by VID of groups, and are building the VLAN group. Namely, in this example, VID belongs to VLAN of "VA" terminal unit T1-1, T2-1, T4-1, T12, and T13, VID belongs to VLAN of "VB" terminal unit T1-2, T3-1, T4-2, T12, and T13, VID belongs to VLAN of "VC" terminal unit T1-3 and T3-2, T4-3, T11, and T13, and terminal unit T1-4, T2-2, T3-3, T13, and T14 assume that VID belongs to VLAN of "VD." Therefore, the port of each bridge BR1-BR4 has taken the composition corresponding to VLAN of the group to whom the connected terminal unit belongs.

[0021]Direct continuation of server VAS/VBS is carried out to ATM network 10 by the server having the function of an address solution server and a multiple address server. Server VAS/VBS is made to correspond to the MAC Address and ATM address of the bridges BR1-BR4 and the ATM terminal equipment T11-T14 by which direct continuation is carried out to ATM network 10, as shown in Table 1. The flag bit (BR flag) which shows that it is a bridge which accommodates branch line LAN belonging to two or more groups, The above-mentioned bridge and ATM terminal equipment have a first address table that registers VID showing the VLAN group who belongs, and can be using for use of each bridge BR1-BR4 and the ATM terminal equipment T11-T14.
[0022]
[Table 1]

MAC アドレス	ATM アドレス	BR フラグ	VID (仮想LAN識別子)
T1	A1	1	VA+VB+VC+VD
T2	A2	1	VA+VD
T3	A3	1	VB+VC+VD
T4	A4	1	VA+VB+VC
T11	A11	0	VC
T12	A12	0	VA+VB
T13	A13	0	VA+VB+VC+VD
T14	A14	0	VD
:	:	:	:

In Table 1, + shown in VID shows the logical sum of each group to whom the bridges BR1-BR4 and the ATM terminal equipment T11-T14 belong.
[0023]This server VAS/VBS is also other terminal units and equipment which has a communication function similarly, and a predetermined MAC Address and ATM address are set up. In this example, the inquiry of the ATM address of a destination device (a bridge or ATM terminal equipment) performed by an address solving request frame is received in advance of data communications, Server VAS/VBS returns the predetermined response by an address solution answer frame to the equipment which performed the inquiry so that data communications can be performed only between the terminal units (terminal unit of the group same in an working example) by which searched the above-mentioned address table and the communication permission was carried out.
[0024]In the case of multiple address frame relay processing, from a transmission source device (a bridge or ATM terminal equipment) to the multiple address frame

transmitted to server VAS/VBS server VAS/VBS, Multiple address frame transmission within a group is performed by transmitting the above-mentioned multiple address frame to all the bridges and ATM terminal equipment which search the 1st address table of the above and belong to the same VLAN as a transmission source device. The address unknown (unknown) frame with which the ATM address solution other than the frame specified in specific address fields, such as a multicast frame and a broadcast frame, is not made is also contained in the above-mentioned multiple address frame.

[0025]Thus, the ATM connection with a bridge and ATM terminal equipment is established fixed so that server VAS/VBS can be accessed from any VLAN of a group. An address solution server and a multiple address server may be constituted from server VAS/VBS which consists of one hardware physically as mentioned above, and it may be made to distribute on ATM network 10, and they may be connected independently. However, to make it distribute, an address solution server and a multiple address server need to have the 1st address table of the above independently.

[0026]The frame format of AAL5 (ATM adaptation layer 5) frame of the LAN emulation standardized by ATM Forum is used for the address solving request frame in this example, an address solution answer frame, and a multiple address frame. The point of having added change in the present invention about the above-mentioned frame format is a point that a server and a bridge add a VID value to an address solving request frame and a multiple address frame.

[0027]That is, as shown in the frame format of Fig.2, the above-mentioned VID value is mapped in the CPCS UU field in the CPCS PDU trailer of five AALs. By being able to use the above-mentioned CPCS UU field for discernment between users, and using this field, Compatibility with existing ATM terminal equipment can be maintained without invading the CPCS PDU payload part in which the data of a transmitting agency, the MAC Address of an address, an ATM address, etc., etc. is stored. About the LAN terminal equipment connected to branch line LAN, it is not necessary to add change at all in this example.

[0028]Here, if a virtual LAN system is built on a large scale, the registration entry of the address table in server VAS/VBS will become huge, and the load in respect of management of a server will become largely. So, in order to make the registration entry of the address table in server VAS/VBS into the minimum, it is desirable to register locally the address of the terminal unit connected to the branch line LAN side port of a bridge on the table of each bridge, without registering with the above-mentioned table.

[0029]In this example, it shall have an address table (henceforth a "LAN address table") which registers locally the address of the terminal unit connected to the branch line LAN side port of self-equipment in each bridge BR1-BR4. Since the LAN address table of these bridges BR1-BR4 is the same composition, it is represented here and shows an example of the LAN address table of bridge BR1 in Table 2.

[0030]

[Table 2]

MAC アドレス	LAN PORT	VID
T1-1	1	VA
T1-2	2	VB
T1-3	3	VC
T1-4	4	VD
:	:	:

[0031]The MAC Address of terminal unit T1-1 - T1-4, the number of the branch line LAN side port (LAN PORT) of bridge BR1 to which the above-mentioned terminal unit is connected, and the VID value of the group to whom the above-mentioned terminal unit belongs are corresponded and registered into this LAN address table.
[0032]Each bridge BR1-BR4 has an address table (henceforth an "ATM address table") for managing the destination address by the side of an ATM network. Since the ATM address table of these bridges BR1-BR4 is the same composition, it is represented here and shows an example of the ATM address table of bridge BR1 in Table 3.
[0033]
[Table 3]

MAC アドレス	ATM アドレス	VCI	VID
T2-2	A2	VC1-2	VD
T3-1	A3	VC1-3	VB
T3-3	A3	VC1-3	VD
T4-1	A4	VC1-4	VA
T4-2	A4	VC1-4	VB
T12	A12	VC1-12	VA+VB
T13	A13	VC1-13	VA+VB+VC+VD
T14	A14	VC1-14	VD
:	:	:	:

The MAC Address of destination terminal equipment, the ATM address, ATM connection VCI established to destination terminal equipment, and the VID value of the group to whom the above-mentioned terminal unit belongs are corresponded and registered into this ATM address table.
[0034]By administration terminal equipment predetermined [on a network] with a VLAN group to SNMP (simple network management protocol), or other means, It is possible to perform operation of registering and deleting VID, to the address table of server VAS/VBS and the ATM address table of each bridge, and, thereby, an address table can be set up.
[0035]Next, the communication operation of the virtual LAN system shown in Fig.1 is described based on the flow chart of Fig.3 thru/or Fig.5.To communication between terminal units, it may carry out between ATM terminal equipment between LAN terminal equipment and ATM terminal equipment and between LAN terminal equipment, and there is a case of the communication from ATM terminal equipment or LAN terminal equipment in multiple address frame relay processing at it. Hereafter, it describes about the working example in these cases.
[0036]First, when communicating from the terminal unit T11 to the terminal unit T13 between ATM terminal equipment as the 1st working example, the transmission source terminal T11 precedes performing communication to the destination terminal equipment T13, and needs to get to know the ATM address of the destination terminal equipment T13. Then, the terminal unit T11 transmits the address solving request frame of the terminal unit T13 including transmitting agency MAC Address T11 and the destination MAC address T13 on the ATM connection to server VAS/VBS established previously.
[0037]If the above-mentioned address solving request frame is received, server VAS/VBS will perform reception operation shown in Fig.3. That is, server VAS/VBS searches whether the destination MAC address T13 in the above-mentioned frame is registered into the first address table of Table 1 (Step 101). When the destination MAC

address is not registered into a first address table, here, The above-mentioned address solving request frame is transmitted to other bridges (when the other when the source of request of the above-mentioned frame is a bridge bridge, and a source of request are ATM terminal equipment, they are all the bridges) (Step 102), and reception operation is ended. In this case, since the destination MAC address T13 is registered into the first address table, The VID value "VA+VB+VC+VD" and source-of-request VID value "VC" which are registered corresponding to above-mentioned MAC Address T13 are compared (Step 103), and it is judged whether there is any common VID value (Step 104).

[0038]Here, since there is a common VID value "VC", it judges that communication of both terminal unit T11 and T13 is permitted, and it is judged whether next the flag bit of the source of request is set (Step 105). And when the flag bit of the above-mentioned source of request is set, while adding VID applicable to an address solution answer frame (Step 106), the above-mentioned address solution answer frame including the ATM address of destination terminal equipment is returned to a source of request (Step 107).

[0039]Since the flag bit of the above-mentioned source of request is not set in the case of this 1st working example, server VAS/VBS, VID returns an address solution answer frame including ATM address A13 of the destination terminal equipment T13 to the terminal unit T11 of a source of request, without adding (Step 107). The terminal unit T11 which received the address solution answer frame can establish the ATM connection to the terminal unit T13 using ATM address A13, and can transmit data on the above-mentioned ATM connection.

[0040]On the other hand, when trying to perform communication to the terminal unit T12 from the terminal unit T11, Since it detects that server VAS/VBS does not have common VID from search of a first address table in Step 104, it judges that the communication between both terminal units is not permitted, and an address solution answer frame is not returned. Therefore, between the terminal unit T11 and T12, it will not be established but the ATM connection can communicate.

[0041]Next, when communicating to the ATM terminal equipment T14 from LAN-terminal-equipment T1-4 connected to bridge BR1 between LAN terminal equipment and ATM terminal equipment as the 2nd working example, Bridge BR1 which received the data frame from terminal unit T1-4 transmits the address solving request frame of the terminal unit T14 on the ATM connection to server VAS/VBS established previously.

[0042]If the above-mentioned address solving request frame is received, server VAS/VBS performs the same reception operation as the 1st working example, searches a first address table, and compares the VID value "VA+VB+VC+VD" of source-of-request bridge BR1 with "VD" of the destination terminal equipment T14. In the 2nd working example, since the common VID value "VD" exists, server VAS/VBS judges that communication of bridge BR1 and the terminal unit T14 is permitted, and returns an address solution answer frame including ATM address A14 of the destination terminal equipment T14 to bridge BR1.

[0043]If an address solution answer frame is received, bridge BR1 will register ATM address A14 and VID value "VD" of the destination terminal equipment T14 into the ATM address table of Table 3, in order to manage the destination address by the side of an ATM network. ATM connection VC1-14 to the terminal unit T14 is established from obtained ATM address A14, and data is transmitted on ATM connection VC1-14. ATM connection VC1-14 established is registered into an ATM address table.

[0044]As mentioned above, by registration of the ATM address to an ATM address table, and a VID value, supposing it receives the transmission frame from LAN-terminal-equipment T1-1 to the ATM terminal equipment T14, for example, bridge BR1 next, Since the ATM connection to the ATM terminal equipment T14 belongs to the VLAN group from whom the transmission destination of what is already established differs, bridge BR1 can discard this transmission frame and it does not need to take out useless traffic to the ATM side by this.

[0045]Next, when communicating to LAN-terminal-equipment T4-3 connected to bridge BR4 from the ATM terminal equipment T11 between ATM terminal equipment and LAN terminal equipment as the 3rd working example, The transmission source terminal T11 transmits the address solving request frame of LAN-terminal-equipment T4-3 to server VAS/VBS. If the above-mentioned address solving request frame is received, although a first address table is searched, server VAS/VBS like the above-mentioned working example, Since the address of LAN-terminal-equipment T4-3 is not registered into the above-mentioned table, the above-mentioned address solving request frame is transmitted to other bridges BR2-BR4 other than source-of-request bridge BR1 connected to ATM network 10 (refer to Step 102 of Fig.3).

[0046]The bridge besides the above has the table shown in Table 2 and 3, the same LAN address table, and an ATM address table, The bridge which received the address solving request frame transmitted [above-mentioned] searches the LAN address table of self-equipment, and judges whether destination terminal equipment is registered. Only bridge BR4 [and] into which the address of LAN-terminal-equipment T4-3 used as an inquiry object is registered in this 3rd working example, The VID value "VC" of terminal unit T4-3 is added to the address solution answer frame containing ATM address A4 of self-equipment, and it returns to server VAS/VBS.

[0047]If the above-mentioned address solution answer frame is received, server VAS/VBS will perform reception operation shown in Fig.4. Namely, the VID value "VC" of the terminal unit T11 of a source of request with which server VAS/VBS is registered into the first address table, The VID value "VC" of destination-terminal-equipment T4-3 added to the address solution answer frame is compared (Step 201), and it is judged whether there is any common VID value (Step 202).

[0048]Server VAS/VBS ends the above-mentioned reception operation, when there is no common VID value, but in this 3rd working example, since the common VID value "VC" exists, communication of both terminal units is judged that a permission is granted. And it is judged whether the flag bit of the source of request is set (Step 203). Here, since the above-mentioned flag bit of the terminal unit T11 is not set, VID of the above-mentioned address solution answer frame is deleted (Step 204), and the address solution answer frame containing ATM address A4 is returned to the terminal unit T11 of a source of request (Step 205).

[0049]The terminal unit T11 which received the address solution answer frame can establish the ATM connection to bridge BR4 using ATM address A4, and can transmit a data frame on the above-mentioned ATM connection. At the time of reception of the above-mentioned data frame, bridge BR4 can search the LAN address table of self-equipment, and it can relay the above-mentioned data frame to the port 3 where LAN-terminal-equipment T4-3 is connected.

[0050]Next, when communicating to LAN-terminal-equipment T4-1 connected to bridge BR4 from LAN-terminal-equipment T1-1 connected to bridge BR1 between LAN terminal equipment as the 4th working example, Bridge BR1 which received the data frame from LAN-terminal-equipment T1-1 transmits the address solving request frame of terminal unit T4-1 to server VAS/VBS like the 2nd working example.

[0051]If the above-mentioned address solving request frame is received, since the address of LAN-terminal-equipment T4-1 is not registered into a first address table, server VAS/VBS will transmit the above-mentioned address solving request frame to other bridges like the 3rd working example. Bridge BR4 which received the address solving request frame transmitted [above-mentioned] searches the LAN address table of self-equipment, adds the VID value "VA" of terminal unit T4-1 to the address solution answer frame containing ATM address A4 of self-equipment, and returns it to server VAS/VBS.

[0052]Server VAS/VBS which received the above-mentioned address solution answer frame compares the VID value "VA+VB+VC+VD" of source-of-request bridge BR1 registered into the first address table with the VID value "VA" of destination-terminal-equipment T4-1 added to the address solution answer frame. In this case, since the VID value "VA" with common server VAS/VBS exists, it judges that communication of both terminal unit T1-1 and T4-1 is permitted, and the address solution answer frame sent from bridge BR4 is transmitted to bridge BR1.
[0053]Bridge BR1 which received the above-mentioned address solution answer frame registers the VID value "VA" into the ATM address table with ATM address A4 corresponding to destination-terminal-equipment T4-1. ATM connection VC1-4 to bridge BR4 is established from obtained ATM address A4, and the data frame received from terminal unit T1-1 is relayed on ATM connection VC1-4. ATM connection VC1-4 established is registered into an ATM address table.
[0054]Bridge BR4 can search the LAN address table of self-equipment at the time of reception of the above-mentioned data frame, and it can relay the above-mentioned data frame to the port 1 where LAN-terminal-equipment T4-1 is connected. Unless registration of the above-mentioned table is erased, the data transmission to the destination terminal equipment once registered into the ATM address table can use this, and does not need to follow the above-mentioned procedure for address solution again.
[0055]Next, it describes about relay processing operation of a multiple address frame. First, when the ATM terminal equipment T12, for example, a terminal unit, sends a multiple address frame as the 5th working example, the transmission source terminal T12 transmits the above-mentioned multiple address frame on the ATM connection to server VAS/VBS established previously. If the above-mentioned multiple address frame is received, server VAS/VBS will perform relay processing operation shown in Fig.5. That is, server VAS/VBS searches a first address table and judges whether the flag bit is set from transmitting agency MAC Address T12 in the above-mentioned frame (Step 301).
[0056]When the above-mentioned flag bit is set, here, Although the transmitting origin VID added into the above-mentioned multiple address frame is identified (Step 302), in the 5th working example, Since the above-mentioned flag bit is not set, the transmitting origin VID from a first address table. That is, while detecting the VLAN group "VA+VB" to whom the terminal unit T12 belongs (Step 303), it belongs to these groups and ATM terminal equipment or a bridge with common VID is searched (Step 304). In this example, all the bridges BR1-BR4 will have accommodated branch line LAN belonging to the group of "VA" or "VB", and only the terminal unit T13 will belong to the above-mentioned group with ATM terminal equipment.
[0057]Next, server VAS/VBS searches a first address table and judges whether the flag bit of the destination BR1-BR4, i.e., bridges, or the terminal unit T13 is set (Step 305). Here, server VAS/VBS adds and relays VID "VA+VB" of the transmission source terminal T12 to the above-mentioned multiple address frame about the bridges BR1-BR4 with which the flag bit of the above-mentioned table is set (Step 306). When acting as intermediary, may use the ATM connection of the point Thu point previously established between a server and each bridge, and, Or the ATM connection of the point Thu multipoint previously established between a server and all the bridges in an ATM network may be used (when using the latter ATM connection, it always becomes the simultaneous transmissive communication to all the bridges).
[0058]Server VAS/VBS about the terminal unit T13 with which the flag bit of the above-mentioned table is cleared, It acts as intermediary using the ATM connection of the point Thu point established previously, without adding VID "VA+VB" of the transmission source terminal T12 to the above-mentioned multiple address frame. The bridge which received the multiple address frame relayed [above-mentioned] searches a LAN address table based on VID added to the above-mentioned multiple address frame, and transmits the above-mentioned multiple address frame only to the LAN

terminal equipment belonging to the above VID. Namely, when Fig.1 is referred to, in bridge BR1, Only to terminal unit T1-1 and T1-2 connected to branch line LAN side ports 1 and 2, in bridge BR2, Only to terminal unit T2-1 connected to branch line LAN side port 1, in bridge BR3, Only as opposed to terminal unit T3-1 connected to branch line LAN side port 1, the above-mentioned multiple address frame is relayed by bridge BR4 only to terminal unit T4-1 and T4-2 which were connected to branch line LAN side ports 1 and 2.

[0059]Next, when LAN-terminal-equipment T3-3 connected to LAN-terminal-equipment, for example, bridge BR, 3 as the 6th working example sends a multiple address frame, Bridge BR3 which received the above-mentioned multiple address frame searches the LAN address table of self-equipment, and it detects VID "VD" of branch line LAN to which terminal unit T3-3 is connected. And bridge BR3 adds detected VID "VD" to a multiple address frame, and it transmits to server VAS/VBS.

[0060]When the above-mentioned multiple address frame is received, server VAS/VBS, While recognizing that it is the multiple address in a VLAN group "VD" from the transmitting origin VID which detected that the flag bit was set in a first address table like the 5th working example, and was added to the above-mentioned multiple address frame, Bridge BR1 belonging to the above-mentioned group "VD", BR2 and the ATM terminal equipment T13, and T14 are discriminated from a first address table.

[0061]Next, server VAS/VBS receives bridge BR1 to which the flag bit of the first address table is set, and BR2, To the terminal unit T13 which adds the transmitting agency VID "VD" to the above-mentioned multiple address frame and with which the flag bit of the above-mentioned table is cleared, and T14, it acts as intermediary, without adding the transmitting agency VID to the above-mentioned multiple address frame.

[0062]Bridge BR1 which received the multiple address frame relayed [above-mentioned], and BR2 search a LAN address table based on VID added to the above-mentioned multiple address frame, and they relay the above-mentioned multiple address frame only to LAN-terminal-equipment T1-4 and T2-2 belonging to the above VID. Therefore, it makes it possible to connect the ATM terminal equipment or the bridge belonging to two or more groups on an ATM network in this example, All the ATM terminal equipment or bridges on a network, Since group management is carried out under control of a server, and there are few parameters which should be managed by the terminal side and they end compared with the method which used the conventional ELAN, the load of the group management in the bridge or ATM terminal equipment belonging to two or more groups can be reduced.

[0063]In this example, since management of the connection established between a server, and each ATM terminal equipment and a bridge becomes easy using a pair of thing, an address solution server and a multiple address server, While making resources, such as an address solution server by the side of a network, and a multiple address server, into the minimum, establishment and band utilization of an efficient connection can be performed.

[0064]Since what is necessary will just be to establish a single connection using signaling processing and communication will be performed only on the above-mentioned connection in this example if it is communication between the same ATM terminal equipment and a bridge physically, Interconnectivity with the existing terminal unit can be maintained without making special processing perform to the conventional terminal unit. The present invention also about the address of not only the above-mentioned working example but the LAN terminal equipment connected to branch line LAN, for example, It is possible to also make it register with the first address table of a server, in this case, it becomes unnecessary for a server to transmit an address solving request frame to a bridge, and the group management of all the terminals on a network of it becomes possible in a server.

[0065]It is also possible to overlap and assign two or more VLAN groups to one port of a bridge in the present invention, and it is also possible to connect two or more terminal units to one port. Although it is the logically independent thing between VLAN(s) in this example, not only this but the thing set up to communicate between specific VLAN(s) is possible for the present invention.

[0066]

[Effect of the Invention]As described above, while carrying out direct continuation of the repeating installation which has two or more ports where the 1st terminal unit is connected, respectively, and a bridge function in the present invention, and the 2nd terminal unit via a trunk network, In the system which performs data communications between the terminal units by which carried out the group division of each port and the second terminal unit of the aforementioned repeating installation, and set up the virtual network, and the communication permission was carried out to the transmission source terminal, The address information of the aforementioned repeating installation and the 2nd terminal unit, and at least one group identification information to which this repeating installation and the 2nd terminal unit belong, The memory response means which has the 1st address storage section that makes the bit information which shows that it is the repeating installation to which several 1st terminal units with which at least one differs in the aforementioned group who does a group are connected correspond, and memorizes it, To the inquiry of the network address of an address which connects to the aforementioned trunk network and is performed in advance of the aforementioned data communications, the aforementioned memory response means, Since a predetermined response is returned to the equipment which performed the aforementioned inquiry so that data communications can be performed only between the terminal units by which searched the 1st above-mentioned address storage section, and the communication permission was carried out [aforementioned], while being able to reduce the load of the group management in the bridge or ATM terminal equipment belonging to two or more groups, Interconnectivity with the existing terminal unit can be maintained without making special processing perform to the conventional terminal unit.

[0067]In Claim 4, to an inquiry of the network address of the address which is not memorized by said 1st address storage section, the aforementioned memory response means, To repeating installation and the 2nd terminal unit other than the equipment which performed this inquiry, transmit this inquiry, and to them the aforementioned repeating installation, Have the 2nd address storage section that makes the MAC Address of the 1st terminal unit connected to self-equipment, and the group identification information to which this each 1st terminal unit belongs correspond, and memorizes them, and an inquiry of the address of this 1st terminal unit is received, The 2nd address storage section is searched, and since the predetermined response include the group identification information corresponding to a corresponding address is returned to the aforementioned memory response means, the load of the group management in the bridge belonging to two or more groups can be reduced.

[0068]In Claim 5, the repeating installation which performed the aforementioned inquiry, The network address of the address obtained by the predetermined response from the aforementioned memory response means, As opposed to the address of the transmission frame from the 1st terminal unit that has the 3rd address storage section that corresponds and memorizes the group identification information to which this address belongs, and was connected to self-equipment, This 3rd address storage section is searched, and since this transmission frame is sent out to the aforementioned trunk network only when communication is permitted between the group to whom an address belongs, and the group to whom the 1st terminal unit concerned belongs, the load of the group management in the bridge belonging to two or more groups can be reduced.

[0069]In Claim 6 and 9, the aforementioned memory response means or a multiple address means, When the frame which should be carried out the multiple address is received, from the group identification descriptor added to the search results or this multiple address frame of the 1st above-mentioned address storage section, Since this multiple address frame is transmitted to the repeating installation or the second terminal unit of the group to whom it was added by the address concerned only when communication is permitted among the groups to whom the group to whom a transmitting agency belongs is judged and this transmitting origin belongs, While making resources, such as an address solution server by the side of a network, and a multiple address server, into the minimum, establishment and band utilization of an efficient connection can be performed.

[0070]As opposed to the multiple address frame from the 1st terminal unit by which the aforementioned repeating installation was connected to self-equipment in Claim 8 and 12, Search the 2nd above-mentioned address storage section, and the multiple address frame which added the group identification information to which this 1st terminal unit belongs is sent out to the aforementioned memory response means, The multiple address frame transmitted from this memory response means is received, Since this multiple address frame is relayed only to the first terminal unit that searches the 2nd above-mentioned address storage section, and belongs to this group based on the group identification information added to this multiple address frame, establishment and band utilization of an efficient connection can be performed.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a configuration diagram showing the composition of one working example of the virtual LAN system using the virtual network management method concerning the present invention.
[Drawing 2]It is a frame format which shows the composition of the frame used for the system of Fig.1.
[Drawing 3]It is a flow chart for describing the operation at the time of the address solving request frame reception of the server shown in Fig.1.
[Drawing 4]It is a flow chart for similarly describing the operation at the time of the address solution answer frame reception of a server.
[Drawing 5]It is a flow chart for similarly describing the operation at the time of the multiple address frame reception of a server.
[Explanations of letters or numerals]
10 ATM network
VAS/ABS Server
BR1-BR4 Bridge
T11 - T14 ATM-terminal equipment
T1-1 - T1-4, T2-1, T2-2, T3-1 - T3-3, T4-1 - T4-3 LAN terminal equipment

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－270803

(43)公開日　平成９年(1997)10月14日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	12/28		9466－5K	Ｈ０４Ｌ	11/20	D	
	12/46			Ｈ０４Ｑ	3/00		
	12/66			Ｈ０４Ｌ	11/00	３１０Ｃ	
Ｈ０４Ｑ	3/00		9466－5K		11/20	B	

審査請求　未請求　請求項の数12　ＯＬ　（全 13 頁）

(21)出願番号　特願平8－80005

(22)出願日　平成８年(1996)４月２日

(71)出願人　000005290
古河電気工業株式会社
東京都千代田区丸の内２丁目６番１号

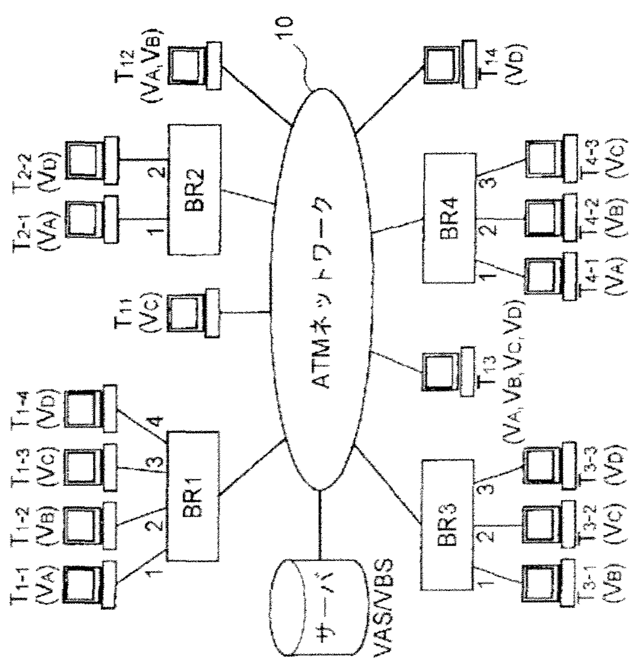
(72)発明者　堀口　政則
東京都千代田区丸の内２丁目６番１号　古河電気工業株式会社内

(72)発明者　鈴木　敦彦
東京都千代田区丸の内２丁目６番１号　古河電気工業株式会社内

(74)代理人　弁理士　長門　侃二

(54)【発明の名称】　仮想ネットワーク構築方法

(57)【要約】
【課題】　複数のグループに属するブリッジ又はＡＴＭ端末装置におけるグループ管理の負荷を低減する。
【解決手段】　ＬＡＮ端末がそれぞれ接続されるブリッジＢＲ1～ＢＲ4及びＡＴＭ端末Ｔ11～Ｔ14をＡＴＭネットワーク１０に直結させ、各端末をグループ分けしてＶＬＡＮの設定を行い、送信元端末と通信許可された端末間でデータ通信を行うシステムにおいて、ブリッジ及びＡＴＭ端末のアドレス情報とグループ識別情報とを、サーバＶＡＳ／ＶＢＳ内の第１のアドレステーブルに対応させて登録し、サーバはデータ通信に先立って行われる宛先のＡＴＭアドレスの問い合わせに対して、第１のアドレステーブルを検索して通信許可された端末間でのみデータ通信が行えるように、応答フレームを問い合わせを行った装置に返す。



【特許請求の範囲】

【請求項１】 第１端末装置がそれぞれ接続される複数のポートとブリッジ機能とを有する中継装置と、第２端末装置とを幹線ネットワークを介して直接接続させるとともに、前記中継装置の各ポート及び第２端末装置をグループ分けして仮想ネットワークの設定を行い、送信元端末装置と通信許可された前記端末装置間でデータ通信を行うシステムにおいて、

前記中継装置及び第２端末装置のアドレス情報と、該中継装置及び第２端末装置が属する少なくとも１つのグループ識別情報と、前記属するグループが少なくとも１つ異なる複数の第１端末装置が接続される中継装置であることを示すビット情報とを対応させて記憶する第１アドレス記憶部を有する記憶応答手段を、前記幹線ネットワークに接続させ、

前記データ通信に先立って行われる宛先のネットワークアドレスの問い合わせに対して、前記記憶応答手段は、前記第１アドレス記憶部を検索して前記通信許可された端末装置間でのみデータ通信が行えるように、所定の応答を前記問い合わせを行った装置に返すことを特徴とする仮想ネットワーク構築方法。

【請求項２】 前記幹線ネットワークは、ＡＴＭネットワークからなり、前記ネットワークアドレスは、ＡＴＭアドレスからなり、前記第１アドレス記憶部に記憶されたアドレス情報は、前記中継装置及び第２端末装置のＭＡＣアドレスと、該ＭＡＣアドレスに対応するＡＴＭアドレスとからなることを特徴とする請求項１に記載の仮想ネットワーク構築方法。

【請求項３】 前記記憶応答手段は、前記問い合わせを行った装置のアドレスに対応したグループ識別情報を、前記第１アドレス記憶部から検索し、該問い合わせを行った装置が所属するグループと、該問い合わせの宛先装置が属するグループとの間で通信が許可されている場合のみ前記所定応答を、該問い合わせを行った装置に返すことを特徴とする請求項１に記載の仮想ネットワーク構築方法。

【請求項４】 前記第１アドレス記憶部に記憶されていない宛先のネットワークアドレスの問い合わせに対して、前記記憶応答手段は、該問い合わせを行った装置以外の前記中継装置及び第２端末装置に、該問い合わせを転送し、

前記中継装置は、自装置に接続された各第１端末装置のＭＡＣアドレスと、該各第１端末装置が属するグループ識別情報とを対応させて記憶する第２アドレス記憶部を有し、該第１端末装置のアドレスの問い合わせに対して、第２アドレス記憶部を検索し、該当アドレスに対応するグループ識別情報を含んだ所定応答を、前記記憶応答手段に返すことを特徴とする請求項１又は３に記載の仮想ネットワーク構築方法。

【請求項５】 前記問い合わせを行った中継装置は、前記記憶応答手段からの所定応答により得られた宛先のネットワークアドレスと、該宛先の属するグループ識別情報とを対応して記憶する第３アドレス記憶部を有し、自装置に接続された第１端末装置からの送信フレームの宛先に対して、該第３アドレス記憶部を検索し、宛先が属するグループと当該第１端末装置が属するグループ間で通信が許可されている場合のみ、該送信フレームを前記幹線ネットワークに送出することを特徴とする請求項１又は３に記載の仮想ネットワーク構築方法。

【請求項６】 前記記憶応答手段は、同報すべきフレームを受信した場合、前記第１アドレス記憶部の検索結果もしくは該同報フレームに付加されたグループ識別子より、送信元が属するグループを判断し、該送信元が属するグループ間で通信が許可されている場合のみ、該同報フレームを当該宛先に付加されたグループの中継装置又は第２端末装置に転送することを特徴とする請求項１，３又は４に記載の仮想ネットワーク構築方法。

【請求項７】 前記記憶応答手段は、前記同報フレームを転送する場合、前記第１アドレス記憶部を検索し、該同報フレームの転送先が、前記属するグループが少なくとも１つ異なる複数の第１端末装置が接続される中継装置の時は、送信元のグループ識別情報を該同報フレームに付加して転送することを特徴とする請求項４又は６に記載の仮想ネットワーク構築方法。

【請求項８】 前記中継装置は、自装置に接続された第１端末装置からの同報フレームに対して、前記第２アドレス記憶部を検索し、該第１端末装置が属するグループ識別情報を付加した同報フレームを前記記憶応答手段に送出し、

また該記憶応答手段から転送されてきた同報フレームに対しては、該同報フレームに付加されたグループ識別情報に基づいて、前記第２アドレス記憶部を検索し、該グループに属する第１端末装置にのみ該同報フレームを中継することを特徴とする請求項４，６又は７に記載の仮想ネットワーク構築方法。

【請求項９】 第１端末装置がそれぞれ接続される複数のポートとブリッジ機能とを有する中継装置と、第２端末装置とを幹線ネットワークを介して直接接続させるとともに、前記中継装置の各ポート及び第２端末装置をグループ分けして仮想ネットワークの設定を行い、送信元端末装置と通信許可された端末装置間でデータ通信を行うシステムにおいて、

前記中継装置及び第２端末装置のアドレス情報と、該中継装置及び第２端末装置が属する少なくとも１つのグループ識別情報と、前記属するグループが少なくとも１つ異なる複数の第１端末装置が接続される中継装置であることを示すビット情報とを対応させて記憶する第１アドレス記憶部を有する同報手段を、前記幹線ネットワークに接続させ、

前記同報手段は、同報すべきフレームを受信した場合、

前記第１アドレス記憶部の検索結果もしくは該同報フレームに付加されたグループ識別子より、送信元が属するグループを判断し、該送信元が属するグループ間で通信が許可されている場合のみ、該同報フレームを当該宛先に付加されたグループの中継装置又は第２端末装置に転送することを特徴とする仮想ネットワーク構築方法。

【請求項１０】　前記幹線ネットワークは、ＡＴＭネットワークからなり、前記ネットワークアドレスは、ＡＴＭアドレスからなり、前記第１アドレス記憶部に記憶されたアドレス情報は、前記中継装置及び第２端末装置のＭＡＣアドレスと、該ＭＡＣアドレスに対応するＡＴＭアドレスとからなることを特徴とする請求項９に記載の仮想ネットワーク構築方法。

【請求項１１】　前記同報手段は、前記同報フレームを転送する場合、前記第１アドレス記憶部を検索し、該同報フレームの転送先が、前記属するグループが少なくとも１つ異なる複数の第１端末装置が接続される中継装置の時は、送信元のグループ識別情報を該同報フレームに付加して転送することを特徴とする請求項９に記載の仮想ネットワーク構築方法。

【請求項１２】　前記中継装置は、自装置に接続された各第１端末装置のＭＡＣアドレスと、該各第１端末装置が属するグループ識別情報とを対応させて記憶する第２アドレス記憶部を有し、自装置に接続された第１端末装置からの同報フレームに対して、前記第２アドレス記憶部を検索し、該第１端末装置が属するグループ識別情報を付加した同報フレームを前記記憶応答手段に送出し、また該記憶応答手段から転送されてきた同報フレームに対しては、該同報フレームに付加されたグループ識別情報に基づいて、前記第２アドレス記憶部を検索し、該グループに属する第１端末装置にのみ該同報フレームを中継することを特徴とする請求項９又は１１に記載の仮想ネットワーク構築方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＡＴＭ（非同期転送モード）ネットワーク等の幹線ネットワークに中継装置を介して接続される複数の端末装置間で、仮想的にグループ化された仮想ＬＡＮを構築する仮想ネットワーク構築方法に関する。

【０００２】

【関連する背景技術】従来、ネットワークにおける端末装置の位置或いはこれら端末装置間の配線といった物理的な構成に関係なく、営業部門、開発部門、研究部門といったワークグループ単位でＬＡＮを構築する技術が、例えば日経コミュニケーション第１８６号（１９９４年１１月２１日発行）に記載された「突入，バーチャルＬＡＮ」等で知られている。これらのＬＡＮは、論理的なグループ分けに基づいてネットワークを構築することから、仮想（バーチャル）ＬＡＮと呼ばれている。

【０００３】上記仮想ＬＡＮを構築する手段としては、複数のＬＡＮポートを持つブリッジ（スイッチングＨＵＢともいう）を用いて、ブリッジの各ＬＡＮポート毎にワークグループ固有の仮想ＬＡＮ識別子（以下、「ＶＩＤ」という）を割り当てる方法があった。しかし、この方法では接続される端末装置の増加に対処できなかった。

【０００４】そこで、従来では、ＡＴＭフォーラムで標準化されているＬＡＮエミュレーションを用いて、例えばＩＥＥＥ８０２．３やＩＥＥＥ８０２．５の規格に準拠した複数のＬＡＮを構成する端末装置を、ブリッジを介して高速のＡＴＭネットワークに接続し、上記ＡＴＭネットワーク上に構築された複数のＥＬＡＮ（エミュレートされたＬＡＮ）に、前述のワークグループに相当する仮想ＬＡＮを対応させて運用する方法があった。この方法では、各ＥＬＡＮ毎に対応するアドレス解決サーバや同報サーバが設けられており、アドレス解決サーバには、該当するＥＬＡＮに所属する端末装置やブリッジのＭＡＣアドレス（物理アドレス）とＡＴＭアドレスが対になって登録されている。

【０００５】この方法では、ユニキャスト通信を行う場合には、予め端末装置が宛先のＡＴＭアドレスを、アドレス解決サーバに問い合わせることで、宛先装置へのコネクションをもち、宛先装置への通信を可能にしていた。また、マルチキャスト通信を行う場合には、送信元から同報サーバに転送されたフレームを、同報サーバが該当するＥＬＡＮに属する全端末装置及びブリッジに転送することによって、グループ内でのマルチキャスト転送を行っていた。

【０００６】

【発明が解決しようとする課題】ところが、上記方法では、ＡＴＭネットワークに直接接続された端末装置（以下、「ＡＴＭ端末装置」という）やブリッジにおいて管理するＥＬＡＮパラメータ、例えば自局アドレス、サーバアドレス、制御系タイマ・カウンタ等がグループ数に比例して大きくなるので、ネットワーク管理面での負荷が大きくなるという問題点があった。

【０００７】また、ネットワーク側では、各グループ毎に対応するアドレス解決サーバや同報サーバを増設しなければならず、製作コストが高くなるという問題点があった。これらサーバの管理とともに、各端末装置側でもサーバとの間にもたれるコネクション（ＡＴＭセルスイッチの接続経路）をグループ毎に管理しなければならず、グループ管理面での負荷が大きくなるという問題点もあった。

【０００８】さらに、物理的に同一のＡＴＭ端末装置とブリッジ間での通信であっても、グループが異なれば、異なるコネクションをシグナリング処理を用いてその都度確立しなければならない。従って、同一のＡＴＭ端末装置とブリッジ間で複数の通信パスが存在する場合に

は、複数のグループに属する端末同士のフレームはどのパスに送信するかという判断処理を行わなければならず、通信処理が煩雑になるという問題点があった。

【0009】また、同報フレームの送信にあたっては、同一のＡＴＭ端末装置とブリッジ間で複数の通信パスが存在する場合には、受信側でフレームが重複して到着することがあるという問題点があった。本発明は、上記問題点に鑑みなされたもので、複数のグループに属するブリッジ又はＡＴＭ端末装置におけるグループ管理の負荷を低減できる仮想ネットワーク構築方法を提供することを目的とする。

【００１０】また、本発明の他の目的は、ネットワーク側におけるアドレス解決サーバ及び同報サーバ等の資源を最小限にするとともに、効率の良いコネクションの確立と帯域利用を行うことにある。さらに、本発明の他の目的は、従来の端末装置に特殊な処理を行わせることなく、既存端末装置との相互接続性を保てる仮想ネットワーク構築方法を提供することにある。

【００１１】

【課題を解決するための手段】上記目的を達成するため、本発明では、第１端末装置がそれぞれ接続される複数のポートとブリッジ機能とを有する中継装置（ブリッジ）と、第２端末装置とを幹線ネットワーク（ＡＴＭネットワーク）を介して直接接続させるとともに、前記ブリッジの各ポート及び第２端末装置をグループ分けして仮想ネットワークの設定を行い、送信元端末装置と通信許可された端末装置間でデータ通信を行うシステムにおいて、ブリッジ及び第２端末装置のＭＡＣアドレスとＡＴＭアドレスのアドレス情報と、ブリッジ及び第２端末装置が属する少なくとも１つのグループ識別情報と、前記属するグループが少なくとも１つ異なる複数の第１端末装置が接続されるブリッジであることを示すビット情報（フラグ）とを対応させて記憶する第１アドレス記憶部（第１アドレステーブル）を有する記憶応答手段（アドレス解決サーバと同報サーバの機能を併せ持つサーバ）を、ＡＴＭネットワークに接続させ、データ通信に先立って行われる宛先のＡＴＭアドレスの問い合わせに対して、サーバは、問い合わせを行った装置のアドレスに対応したグループ識別情報を、第１アドレステーブルから検索して、問い合わせを行った装置が所属するグループと、問い合わせの宛先装置が属するグループとの間で通信が許可されている場合のみ、通信許可された端末装置間でデータ通信が行えるように、所定の応答を前記問い合わせを行った装置に返す。

【００１２】請求項４では、第１アドレステーブルに記憶されていない宛先のＡＴＭアドレスの問い合わせに対して、サーバは、該問い合わせを行った装置以外のブリッジ及び第２端末装置に、該問い合わせを転送し、ブリッジは、自装置に接続される第１端末装置のＭＡＣアドレスと、該各第１端末装置が属するグループ識別情報とを対応させて記憶する第２アドレステーブルを有し、該第１端末装置のアドレスの問い合わせに対して、第２アドレステーブルを検索し、該当アドレスに対応するグループ識別情報を含んだ所定応答をサーバに返す。

【００１３】請求項５では、問い合わせを行ったブリッジは、サーバからの所定応答により得られた宛先のＡＴＭアドレスと、該宛先の属するグループ識別情報とを対応して記憶する第３アドレステーブルを有し、自装置に接続された第１端末装置からの送信フレームの宛先に対して、第３アドレステーブルを検索し、宛先が属するグループと当該第１端末装置が属するグループ間で通信が許可されている場合のみ、送信フレームをＡＴＭネットワークに送出する。

【００１４】請求項６，９では、サーバは、同報すべきフレームを受信した場合、第１アドレステーブルの検索結果もしくは該同報フレームに付加されたグループ識別子より、送信元が属するグループを判断し、該送信元が属するグループ間で通信が許可されている場合のみ、該同報フレームを当該宛先に付加されたグループのブリッジ又は第２端末装置に転送する。

【００１５】請求項８，１２では、中継装置は、自装置に接続された第１端末装置からの同報フレームに対して、前記第２アドレステーブルを検索し、該第１端末装置が属するグループ識別情報を付加した同報フレームをサーバに送出し、またサーバから転送されてきた同報フレームに対しては、該同報フレームに付加されたグループ識別情報に基づいて、前記第２アドレステーブルを検索し、該グループに属する第１端末装置にのみ該同報フレームを中継する。

【００１６】

【発明の実施の形態】本発明に係る仮想ネットワーク構築方法を図１乃至図５の図面に基づいて説明する。図１は、本発明に係る仮想ネットワーク管理方法を用いたバーチャルＬＡＮシステムの一実施例の構成を示す構成図であり、ＡＴＭフォーラム準拠のＬＡＮエミュレーション（既存のＬＡＮ資産をＡＴＭ環境で利用するための仕様）を用いて、バーチャルＬＡＮ（以下、「ＶＬＡＮ」という）を構築した一実施例である。図において、ＶＬＡＮシステムでは、図示しないＡＴＭセルスイッチから構成されるＡＴＭネットワーク１０のような高速ネットワークをバックボーンに有し、複数のブリッジＢＲ1～ＢＲ4、ＡＴＭ端末装置Ｔ11～Ｔ14及びサーバＶＡＳ／ＶＢＳをＡＴＭネットワーク１０に直接接続して構成されている。

【００１７】ブリッジＢＲ1～ＢＲ4は、ＡＴＭネットワーク１０と接続されるＡＴＭネットワーク側ポートと、端末装置が接続される支線ＬＡＮ側ポートをそれぞれ有しており、自装置のポート間、他のブリッジ及びＡＴＭ端末装置とのＡＴＭネットワーク側ポート間でＭＡＣ層レベルでのブリッジング接続を行っている。ブリッジＢ

Ｒ1～ＢＲ4は、ＶＬＡＮの機能を有し、それぞれの支線ＬＡＮ側ポートが独立にどのＶＬＡＮに属するか設定することができ、その際に１つのポートが２つ以上のＶＬＡＮに属するように設定することも可能である。異なるＶＬＡＮは、ＡＴＭネットワーク１０上では、異なるエミュレーティッドＬＡＮ（ＥＬＡＮ）として識別される。これによりＶＬＡＮは、ブリッジＢＲ1～ＢＲ4にまたがって構築することが可能になる。このＶＬＡＮの機能において、異なるＶＬＡＮ間では、マルチキャストパケット（ブロードキャストパケットも含む）は転送されない。

【００１８】ブリッジＢＲ1～ＢＲ4は、複数のグループに属する支線ＬＡＮを収容しており、ブリッジＢＲ1の各支線ＬＡＮ側ポート１～４には各支線ＬＡＮの端末装置（以下、「ＬＡＮ端末装置」という）Ｔ1-1～Ｔ1-4が、ブリッジＢＲ2の各支線ＬＡＮ側ポート１，２にはＬＡＮ端末装置Ｔ2-1，Ｔ2-2が、ブリッジＢＲ3の各支線ＬＡＮ側ポート１～３にはＬＡＮ端末装置Ｔ3-1～Ｔ3-3が、またブリッジＢＲ4の各支線ＬＡＮ側ポート１～３にはＬＡＮ端末装置Ｔ4-1～Ｔ4-3が、それぞれ接続されている。

【００１９】なお、本実施例において、ブリッジＢＲ1～ＢＲ4には、ＭＡＣアドレスＴ1～Ｔ4及びＡＴＭアドレスＡ1～Ａ4がそれぞれ設定されている。また、ＬＡＮ端末装置Ｔ1-1～Ｔ1-4，Ｔ2-1，Ｔ2-2，Ｔ3-1～Ｔ3-3，Ｔ4-1～Ｔ4-3には、上記記号と同じＭＡＣアドレスＴ1-1～Ｔ1-4，Ｔ2-1，Ｔ2-2，Ｔ3-1～Ｔ3-3，Ｔ4-1～Ｔ4-3がそれぞれ設定されている。また、ＡＴＭ端末装置Ｔ11～Ｔ14は、ＡＴＭネットワーク１０と直接接続されており、上記記号と同じＭＡＣアドレスＴ11～Ｔ14及びＡＴＭアドレスＡ11～Ａ14が設定されている。

【００２０】これら端末装置は、ＶＩＤで識別されるいずれかのグループに所属し、ＶＬＡＮグループを構築している。すなわち、本実施例では、端末装置Ｔ1-1，Ｔ2-1，Ｔ4-1，Ｔ12，Ｔ13はＶＩＤが「VA」のＶＬＡＮに属し、端末装置Ｔ1-2，Ｔ3-1，Ｔ4-2，Ｔ12，Ｔ13はＶＩＤが「VB」のＶＬＡＮに属し、端末装置Ｔ1-3，Ｔ3-2，Ｔ4-3，Ｔ11，Ｔ13はＶＩＤが「VC」のＶＬＡＮに属し、端末装置Ｔ1-4，Ｔ2-2，Ｔ3-3，Ｔ13，Ｔ14はＶＩＤが「VD」のＶＬＡＮに属しているものとする。従って、各ブリッジＢＲ1～ＢＲ4のポートは、その接続された端末装置の属するグループのＶＬＡＮに対応した構成をとっている。

【００２１】サーバＶＡＳ／ＶＢＳは、アドレス解決サーバと同報サーバの機能を併せ持つサーバでＡＴＭネットワーク１０と直接接続されている。サーバＶＡＳ／ＶＢＳは、表１に示すように、ＡＴＭネットワーク１０に直接接続されるブリッジＢＲ1～ＢＲ4及びＡＴＭ端末装置Ｔ11～Ｔ14のＭＡＣアドレスとＡＴＭアドレスに対応させて、複数のグループに属する支線ＬＡＮを収容するブリッジであることを示すフラグビット（ＢＲフラグ）と、上記ブリッジ及びＡＴＭ端末装置が所属するＶＬＡＮグループを表すＶＩＤを登録する第１のアドレステーブルを有しており、各ブリッジＢＲ1～ＢＲ4及びＡＴＭ端末装置Ｔ11～Ｔ14の利用に役立てられている。

【００２２】

【表１】

ＭＡＣ アドレス	ＡＴＭ アドレス	ＢＲ フラグ	ＶＩＤ （仮想ＬＡＮ識別子）
T1	A1	1	VA＋VB＋VC＋VD
T2	A2	1	VA＋VD
T3	A3	1	VB＋VC＋VD
T4	A4	1	VA＋VB＋VC
T11	A11	0	VC
T12	A12	0	VA＋VB
T13	A13	0	VA＋VB＋VC＋VD
T14	A14	0	VD
：	：	：	：

なお、表１において、ＶＩＤに示されている＋は、ブリッジＢＲ1～ＢＲ4及びＡＴＭ端末装置Ｔ11～Ｔ14が属する各グループの論理和を示している。

【００２３】このサーバＶＡＳ／ＶＢＳも、他の端末装置と同様に通信機能を有する装置であり、所定のＭＡＣアドレス及びＡＴＭアドレスが設定されている。また、本実施例では、データ通信に先立って、アドレス解決要求フレームによって行われる宛先装置（ブリッジ又はＡＴＭ端末装置）のＡＴＭアドレスの問い合わせに対して、サーバＶＡＳ／ＶＢＳは、上記アドレステーブルを検索して通信許可された端末装置（実施例では、同じグループの端末装置）間でのみデータ通信が行えるように、アドレス解決応答フレームによる所定の応答を、問い合わせを行った装置に返す。

【００２４】また、同報フレーム中継処理の場合、送信元装置（ブリッジ又はＡＴＭ端末装置）からサーバＶＡＳ／ＶＢＳに送信された同報フレームに対して、サーバＶＡＳ／ＶＢＳは、上記第１のアドレステーブルを検索して送信元装置と同じＶＬＡＮに属する全ブリッジ及びＡＴＭ端末装置に、上記同報フレームを転送することによって、グループ内での同報フレーム転送を行う。上記同報フレームには、マルチキャストフレーム、ブロードキャストフレームといった特定のアドレスフィールドで規定されたフレームの他に、ＡＴＭアドレス解決がなされていない宛先不明（アンノウン）フレームも含まれる。

【００２５】このようにサーバＶＡＳ／ＶＢＳは、いずれのグループのＶＬＡＮからもアクセスが可能なように、ブリッジ及びＡＴＭ端末装置とのＡＴＭコネクションが固定的に確立されている。なお、アドレス解決サーバと同報サーバは、上記のように物理的に１つのハードウエアからなるサーバＶＡＳ／ＶＢＳで構成しても良いし、ＡＴＭネットワーク１０上に分散させて別々に接続させても良い。但し、分散させる場合には、アドレス解決サーバ及び同報サーバが、上記第１のアドレステーブルを別々に有する必要がある。

【００２６】本実施例におけるアドレス解決要求フレーム、アドレス解決応答フレーム、同報フレームは、ＡＴＭフォーラムで標準化されているＬＡＮエミュレーションのＡＡＬ５（ＡＴＭアダプテーションレイヤ５）フレームのフレームフォーマットを用いる。上記フレームフォーマットに関して、本発明において変更を加えた点は、サーバ及びブリッジがアドレス解決要求フレーム及び同報フレームにＶＩＤ値を付加する点である。

【００２７】すなわち、図２のフレームフォーマットに示すように、ＡＡＬ５フレームのＣＰＣＳ　ＰＤＵトレイラ中にあるＣＰＣＳ　ＵＵフィールドに、上記ＶＩＤ値をマッピングする。上記ＣＰＣＳ　ＵＵフィールドは、ユーザ間識別に用いることが可能であり、このフィールドを用いることにより、送信元や宛先のＭＡＣアドレス及びＡＴＭアドレス等のデータが格納されているＣＰＣＳ　ＰＤＵペイロード部を侵すことなく、既存ＡＴＭ端末装置との互換性を保つことができる。なお、本実施例では、支線ＬＡＮに接続されるＬＡＮ端末装置に関しては、何ら変更を加える必要はない。

【００２８】ここで、バーチャルＬＡＮシステムが大規

模に構築されると、サーバＶＡＳ／ＶＢＳにおけるアドレステーブルの登録エントリが膨大になって、サーバの管理面での負荷が大きくなる。そこで、サーバＶＡＳ／ＶＢＳにおけるアドレステーブルの登録エントリを最小限にするためには、ブリッジの支線ＬＡＮ側ポートに接続される端末装置のアドレスを、上記テーブルに登録せずに各ブリッジのテーブルによってローカルに登録するのが望ましい。

【００２９】本実施例では、各ブリッジＢＲ1～ＢＲ4において、自装置の支線ＬＡＮ側ポートに接続されている端末装置のアドレスを、ローカルに登録するアドレステーブル（以下、「ＬＡＮアドレステーブル」という）を有するものとする。これらブリッジＢＲ1～ＢＲ4のＬＡＮアドレステーブルは、同様の構成なので、ここでは代表して表２に、ブリッジＢＲ1のＬＡＮアドレステーブルの一例を示す。

【００３０】

【表２】

MAC アドレス	LAN PORT	VID
T1-1	1	VA
T1-2	2	VB
T1-3	3	VC
T1-4	4	VD
：	：	：

【００３１】このＬＡＮアドレステーブルには、端末装置Ｔ1-1～Ｔ1-4のＭＡＣアドレスと、上記端末装置が接続されるブリッジＢＲ1の支線ＬＡＮ側ポート（ＬＡＮ　ＰＯＲＴ）の番号と、上記端末装置が属するグループのＶＩＤ値とが対応して登録されている。

【００３２】また、各ブリッジＢＲ1～ＢＲ4は、ＡＴＭネットワーク側の宛先アドレスを管理するためのアドレステーブル（以下、「ＡＴＭアドレステーブル」という）を有している。これらブリッジＢＲ1～ＢＲ4のＡＴＭアドレステーブルは、同様の構成なので、ここでは代表して表３に、ブリッジＢＲ1のＡＴＭアドレステーブルの一例を示す。

【００３３】

【表３】

ＭＡＣ アドレス	ＡＴＭ アドレス	ＶＣＩ	ＶＩＤ
T2-2	A2	ＶC1-2	VD
T3-1	A3	ＶC1-3	VB
T3-3	A3	ＶC1-3	VD
T4-1	A4	ＶC1-4	VA
T4-2	A4	ＶC1-4	VB
T12	A12	ＶC1-12	VA＋VB
T13	A13	ＶC1-13	VA＋VB＋VC＋VD
T14	A14	ＶC1-14	VD
：	：	：	：

このＡＴＭアドレステーブルには、宛先端末装置のＭＡＣアドレスと、ＡＴＭアドレスと、宛先端末装置に対して確立されたＡＴＭコネクションＶＣＩと、上記端末装置が属するグループのＶＩＤ値とが対応して登録されている。

【００３４】なお、ＶＬＡＮグループでは、ネットワーク上の所定の管理端末装置からＳＮＭＰ（シンプル・ネットワーク・マネージメント・プロトコル）等の手段により、サーバＶＡＳ／ＶＢＳのアドレステーブル及び各ブリッジのＡＴＭアドレステーブルに対して、ＶＩＤを登録・削除する操作を行うことが可能であり、これによりアドレステーブルの設定を行うことができる。

【００３５】次に、図１に示したバーチャルＬＡＮシステムの通信動作を図３乃至図５のフローチャートに基づいて説明する。なお、端末装置間の通信には、ＡＴＭ端末装置間、ＬＡＮ端末装置とＡＴＭ端末装置間、ＬＡＮ端末装置間で行う場合があり、同報フレーム中継処理には、ＡＴＭ端末装置又はＬＡＮ端末装置からの通信の場合がある。以下、これらの場合の実施例について説明する。

【００３６】まず、第１実施例としてＡＴＭ端末装置間、例えば端末装置Ｔ11から端末装置Ｔ13に通信を行う場合、送信元端末装置Ｔ11は、宛先端末装置Ｔ13に対する通信を行うに先立って、宛先端末装置Ｔ13のＡＴＭアドレスを知る必要がある。そこで、端末装置Ｔ11は、予め確立されているサーバＶＡＳ／ＶＢＳへのＡＴＭコネクション上に、送信元ＭＡＣアドレスＴ11、宛先ＭＡＣアドレスＴ13を含んだ端末装置Ｔ13のアドレス解決要求フレームを送信する。

【００３７】上記アドレス解決要求フレームを受信すると、サーバＶＡＳ／ＶＢＳは、図３に示す受信処理動作を行う。すなわち、サーバＶＡＳ／ＶＢＳは、上記フレーム中の宛先ＭＡＣアドレスＴ13が表１の第１のアドレステーブルに登録されているかどうか検索する（ステップ１０１）。ここで、宛先ＭＡＣアドレスが第１のアドレステーブルに登録されていない場合には、他のブリッジ（上記フレームの要求元がブリッジの時にはそれ以外のブリッジ、また要求元がＡＴＭ端末装置の時には全てのブリッジ）に上記アドレス解決要求フレームを転送して（ステップ１０２）、受信処理動作を終了する。この場合には、宛先ＭＡＣアドレスＴ13が第１のアドレステーブルに登録されているので、上記ＭＡＣアドレスＴ13に対応して登録されているＶＩＤ値「VA＋VB＋VC＋VD」と要求元ＶＩＤ値「VC」とを比較し（ステップ１０３）、共通のＶＩＤ値があるかどうか判断する（ステップ１０４）。

【００３８】ここでは、共通のＶＩＤ値「VC」があるので、両端末装置Ｔ11，Ｔ13の通信が許可されると判断し、次に要求元のフラグビットがセットされているかどうか判断する（ステップ１０５）。そして、上記要求元のフラグビットがセットされている場合には、アドレス解決応答フレームに該当するＶＩＤを付加するとともに（ステップ１０６）、宛先端末装置のＡＴＭアドレスを含む上記アドレス解決応答フレームを要求元に返す（ステップ１０７）。

【００３９】なお、この第１実施例の場合には、上記要

求元のフラグビットがセットされていないので、サーバＶＡＳ／ＶＢＳは、ＶＩＤは付加せずに、宛先端末装置Ｔ13のＡＴＭアドレスＡ13を含むアドレス解決応答フレームを、要求元の端末装置Ｔ11に対して返す（ステップ１０７）。アドレス解決応答フレームを受信した端末装置Ｔ11は、ＡＴＭアドレスＡ13を用いて端末装置Ｔ13に対するＡＴＭコネクションを確立し、上記ＡＴＭコネクション上にデータを送信することができる。

【００４０】一方、例えば端末装置Ｔ11から端末装置Ｔ12に対する通信を行おうとした場合には、サーバＶＡＳ／ＶＢＳは、ステップ１０４において第１のアドレステーブルの検索から共通のＶＩＤがないことを検知するので、両端末装置間の通信は許可されないと判断し、アドレス解決応答フレームを返さない。従って、端末装置Ｔ11，Ｔ12間にＡＴＭコネクションは確立されず、通信が行えないこととなる。

【００４１】次に、第２実施例としてＬＡＮ端末装置とＡＴＭ端末装置間、例えばブリッジＢＲ1に接続されたＬＡＮ端末装置Ｔ1-4からＡＴＭ端末装置Ｔ14に通信を行う場合、端末装置Ｔ1-4からのデータフレームを受けたブリッジＢＲ1は、予め確立されているサーバＶＡＳ／ＶＢＳへのＡＴＭコネクション上に、端末装置Ｔ14のアドレス解決要求フレームを送信する。

【００４２】上記アドレス解決要求フレームを受信すると、サーバＶＡＳ／ＶＢＳは、第１実施例と同様の受信処理動作を行い、第１のアドレステーブルを検索し、要求元ブリッジＢＲ1のＶＩＤ値「VA＋VB＋VC＋VD」と宛先端末装置Ｔ14の「VD」を比較する。第２実施例では、共通のＶＩＤ値「VD」が存在することから、サーバＶＡＳ／ＶＢＳは、ブリッジＢＲ1と端末装置Ｔ14の通信が許可されると判断し、宛先端末装置Ｔ14のＡＴＭアドレスＡ14を含むアドレス解決応答フレームを、ブリッジＢＲ1に返す。

【００４３】アドレス解決応答フレームを受信すると、ブリッジＢＲ1は、ＡＴＭネットワーク側の宛先アドレスを管理するために、表３のＡＴＭアドレステーブルに宛先端末装置Ｔ14のＡＴＭアドレスＡ14と、ＶＩＤ値「VD」を登録しておく。また、得られたＡＴＭアドレスＡ14から端末装置Ｔ14に対するＡＴＭコネクションＶＣ1-14を確立し、ＡＴＭコネクションＶＣ1-14上にデータを送信する。なお、確立されたＡＴＭコネクションＶＣ1-14も、ＡＴＭアドレステーブルに登録される。

【００４４】以上のように、ＡＴＭアドレステーブルへのＡＴＭアドレス、ＶＩＤ値の登録により、この後にブリッジＢＲ1が、例えばＬＡＮ端末装置Ｔ1-1からＡＴＭ端末装置Ｔ14への送信フレームを受信したとすると、ＡＴＭ端末装置Ｔ14へのＡＴＭコネクションは既に確立されているものの送信先が異なるＶＬＡＮグループに属するため、ブリッジＢＲ1はこの送信フレームを廃棄することができ、これによって無駄なトラヒックをＡＴＭ側に出さずに済む。

【００４５】次に、第３実施例としてＡＴＭ端末装置とＬＡＮ端末装置間、例えばＡＴＭ端末装置Ｔ11からブリッジＢＲ4に接続されたＬＡＮ端末装置Ｔ4-3に通信を行う場合、送信元端末装置Ｔ11は、サーバＶＡＳ／ＶＢＳに対してＬＡＮ端末装置Ｔ4-3のアドレス解決要求フレームを送信する。上記アドレス解決要求フレームを受信すると、サーバＶＡＳ／ＶＢＳは、上記実施例と同様、第１のアドレステーブルを検索するが、上記テーブルにはＬＡＮ端末装置Ｔ4-3のアドレスが登録されていないため、上記アドレス解決要求フレームを、ＡＴＭネットワーク１０に接続されている要求元ブリッジＢＲ1以外の他のブリッジＢＲ2～ＢＲ4に転送する（図３のステップ１０２参照）。

【００４６】上記他のブリッジは、表２及び表３に示したテーブルと同様のＬＡＮアドレステーブル及びＡＴＭアドレステーブルを有しており、上記転送されてきたアドレス解決要求フレームを受信したブリッジは、自装置のＬＡＮアドレステーブルを検索し、宛先端末装置が登録されているかどうか判断する。そして、この第３実施例では、問い合わせ対象となっているＬＡＮ端末装置Ｔ4-3のアドレスが登録されているブリッジＢＲ4のみが、自装置のＡＴＭアドレスＡ4を含むアドレス解決応答フレームに端末装置Ｔ4-3のＶＩＤ値「VC」を付加してサーバＶＡＳ／ＶＢＳに返す。

【００４７】上記アドレス解決応答フレームを受信すると、サーバＶＡＳ／ＶＢＳは、図４に示す受信処理動作を行う。すなわち、サーバＶＡＳ／ＶＢＳは、第１のアドレステーブルに登録されている要求元の端末装置Ｔ11のＶＩＤ値「VC」と、アドレス解決応答フレームに付加された宛先端末装置Ｔ4-3のＶＩＤ値「VC」とを比較し（ステップ２０１）、共通のＶＩＤ値があるかどうか判断する（ステップ２０２）。

【００４８】サーバＶＡＳ／ＶＢＳは、共通のＶＩＤ値がない場合には、上記受信処理動作を終了するが、この第３実施例では、共通のＶＩＤ値「VC」が存在するので、両端末装置の通信は許可されると判断する。そして、要求元のフラグビットがセットされているかどうか判断する（ステップ２０３）。ここでは、端末装置Ｔ11の上記フラグビットがセットされていないので、上記アドレス解決応答フレームのＶＩＤを削除し（ステップ２０４）、ＡＴＭアドレスＡ4を含むアドレス解決応答フレームを、要求元の端末装置Ｔ11に返す（ステップ２０５）。

【００４９】アドレス解決応答フレームを受信した端末装置Ｔ11は、ＡＴＭアドレスＡ4を用いてブリッジＢＲ4に対するＡＴＭコネクションを確立し、上記ＡＴＭコネクション上にデータフレームを送信することができる。また、ブリッジＢＲ4は、上記データフレームの受信時に、自装置のＬＡＮアドレステーブルを検索し、ＬＡＮ

端末装置Ｔ4-3の接続されているポート３に、上記データフレームを中継することができる。

【００５０】次に、第４実施例としてＬＡＮ端末装置間、例えばブリッジＢＲ1に接続されたＬＡＮ端末装置Ｔ1-1からブリッジＢＲ4に接続されたＬＡＮ端末装置Ｔ4-1に通信を行う場合、ＬＡＮ端末装置Ｔ1-1からのデータフレームを受信したブリッジＢＲ1は、第２実施例と同様、端末装置Ｔ4-1のアドレス解決要求フレームをサーバＶＡＳ／ＶＢＳに送信する。

【００５１】上記アドレス解決要求フレームを受信すると、サーバＶＡＳ／ＶＢＳは、第３実施例と同様、第１のアドレステーブルにＬＡＮ端末装置Ｔ4-1のアドレスが登録されていないため、上記アドレス解決要求フレームを、他のブリッジに転送する。上記転送されてきたアドレス解決要求フレームを受信したブリッジＢＲ4は、自装置のＬＡＮアドレステーブルを検索し、自装置のＡＴＭアドレスＡ4を含むアドレス解決応答フレームに端末装置Ｔ4-1のＶＩＤ値「VA」を付加してサーバＶＡＳ／ＶＢＳに返す。

【００５２】上記アドレス解決応答フレームを受信したサーバＶＡＳ／ＶＢＳは、第１のアドレステーブルに登録されている要求元ブリッジＢＲ1のＶＩＤ値「VA＋VB＋VC＋VD」と、アドレス解決応答フレームに付加された宛先端末装置Ｔ4-1のＶＩＤ値「VA」とを比較する。この場合、サーバＶＡＳ／ＶＢＳは、共通のＶＩＤ値「VA」が存在するので、両端末装置Ｔ1-1，Ｔ4-1の通信は許可されると判断し、ブリッジＢＲ4から送られてきたアドレス解決応答フレームをブリッジＢＲ1に転送する。

【００５３】上記アドレス解決応答フレームを受信したブリッジＢＲ1は、ＡＴＭアドレステーブルに宛先端末装置Ｔ4-1に対応したＡＴＭアドレスＡ4と、ＶＩＤ値「VA」を登録しておく。また、得られたＡＴＭアドレスＡ4からブリッジＢＲ4に対するＡＴＭコネクションＶＣ1-4を確立し、ＡＴＭコネクションＶＣ1-4上に端末装置Ｔ1-1から受信したデータフレームを中継する。なお、確立されたＡＴＭコネクションＶＣ1-4も、ＡＴＭアドレステーブルに登録される。

【００５４】ブリッジＢＲ4は、上記データフレームの受信時に自装置のＬＡＮアドレステーブルを検索し、ＬＡＮ端末装置Ｔ4-1の接続されているポート１に、上記データフレームを中継することができる。なお、一旦ＡＴＭアドレステーブルに登録された宛先端末装置に対するデータ送信は、上記テーブルの登録が抹消されない限り、これを利用することが可能でありアドレス解決のための上記手順を再度行う必要はない。

【００５５】次に、同報フレームの中継処理動作について説明する。まず、第５実施例としてＡＴＭ端末装置、例えば端末装置Ｔ12が同報フレームを発信する場合、送信元端末装置Ｔ12は、予め確立されているサーバＶＡＳ／ＶＢＳへのＡＴＭコネクション上に、上記同報フレームを送信する。上記同報フレームを受信すると、サーバＶＡＳ／ＶＢＳは、図５に示す中継処理動作を行う。すなわち、サーバＶＡＳ／ＶＢＳは、第１のアドレステーブルを検索し、上記フレーム中の送信元ＭＡＣアドレスＴ12からフラグビットがセットされているかどうか判断する（ステップ３０１）。

【００５６】ここで、上記フラグビットがセットされている場合には、上記同報フレーム中に付加された送信元ＶＩＤを識別するが（ステップ３０２）、第５実施例では、上記フラグビットがセットされていないので、第１のアドレステーブルから送信元ＶＩＤ、すなわち端末装置Ｔ12の所属するＶＬＡＮグループ「VA＋VB」を検知するとともに（ステップ３０３）、これらグループに属し、共通のＶＩＤを持つＡＴＭ端末装置又はブリッジを検索する（ステップ３０４）。本実施例では、全てのブリッジＢＲ1～ＢＲ4が「VA」もしくは「VB」のグループに属する支線ＬＡＮを収容しており、ＡＴＭ端末装置では端末装置Ｔ13のみが上記グループに属することになる。

【００５７】次に、サーバＶＡＳ／ＶＢＳは、第１のアドレステーブルを検索し、転送先、すなわちブリッジＢＲ1～ＢＲ4又は端末装置Ｔ13のフラグビットがセットされているかどうか判断する（ステップ３０５）。ここで、サーバＶＡＳ／ＶＢＳは、上記テーブルのフラグビットがセットされているブリッジＢＲ1～ＢＲ4については、上記同報フレームに送信元端末装置Ｔ12のＶＩＤ「VA＋VB」を付加して中継する（ステップ３０６）。なお、中継に際しては、サーバと各ブリッジとの間で予め確立されたポイント・トゥ・ポイントのＡＴＭコネクションを用いても良いし、或いはサーバとＡＴＭネットワーク内の全ブリッジとの間で予め確立されたポイント・トゥ・マルチポイントのＡＴＭコネクションを用いても良い（後者のＡＴＭコネクションを用いる場合は、常に全ブリッジに対する同報通信となる）。

【００５８】また、サーバＶＡＳ／ＶＢＳは、上記テーブルのフラグビットがクリアされている端末装置Ｔ13については、上記同報フレームに送信元端末装置Ｔ12のＶＩＤ「VA＋VB」を付加することなく、予め確立されたポイント・トゥ・ポイントのＡＴＭコネクションを用いて中継する。上記中継された同報フレームを受信したブリッジは、上記同報フレームに付加されたＶＩＤを基にＬＡＮアドレステーブルを検索し、上記ＶＩＤに属するＬＡＮ端末装置にのみ上記同報フレームを送信する。すなわち、図１を参照すると、ブリッジＢＲ1では、支線ＬＡＮ側ポート１，２に接続された端末装置Ｔ1-1，Ｔ1-2に対してのみ、ブリッジＢＲ2では、支線ＬＡＮ側ポート１に接続された端末装置Ｔ2-1に対してのみ、ブリッジＢＲ3では、支線ＬＡＮ側ポート１に接続された端末装置Ｔ3-1に対してのみ、またブリッジＢＲ4では、支

線ＬＡＮ側ポート１，２に接続された端末装置Ｔ4-1，Ｔ4-2に対してのみ、上記同報フレームが中継される。

【００５９】次に、第６実施例としてＬＡＮ端末装置、例えばブリッジＢＲ3に接続されたＬＡＮ端末装置Ｔ3-3が同報フレームを発信する場合、上記同報フレームを受信したブリッジＢＲ3は、自装置のＬＡＮアドレステーブルを検索し、端末装置Ｔ3-3が接続されている支線ＬＡＮのＶＩＤ「VD」を検知する。そして、ブリッジＢＲ3は、検知したＶＩＤ「VD」を同報フレームに付加してサーバＶＡＳ／ＶＢＳに送信する。

【００６０】上記同報フレームを受信すると、サーバＶＡＳ／ＶＢＳは、第５実施例と同様、第１のアドレステーブルにおいてフラグビットがセットされていることを検知して、上記同報フレームに付加された送信元ＶＩＤからＶＬＡＮグループ「VD」内の同報であることを認識するとともに、第１のアドレステーブルから上記グループ「VD」に属するブリッジＢＲ1，ＢＲ2及びＡＴＭ端末装置Ｔ13，Ｔ14を識別する。

【００６１】次に、サーバＶＡＳ／ＶＢＳは、第１のアドレステーブルのフラグビットがセットされているブリッジＢＲ1，ＢＲ2に対しては、上記同報フレームに送信元ＶＩＤ「VD」を付加し、また上記テーブルのフラグビットがクリアされている端末装置Ｔ13，Ｔ14に対しては、上記同報フレームに送信元ＶＩＤを付加せずに中継する。

【００６２】上記中継された同報フレームを受信したブリッジＢＲ1，ＢＲ2は、上記同報フレームに付加されたＶＩＤを基にＬＡＮアドレステーブルを検索し、上記ＶＩＤに属するＬＡＮ端末装置Ｔ1-4，Ｔ2-2にのみ上記同報フレームを中継する。従って、本実施例では、複数グループに属するＡＴＭ端末装置又はブリッジをＡＴＭネットワーク上で接続させることを可能にし、ネットワーク上の全てのＡＴＭ端末装置又はブリッジは、サーバの制御の下にグループ管理されるために、従来のＥＬＡＮを用いた方法に比べて、端末側で管理すべきパラメータが少なくてすむので、複数のグループに属するブリッジ又はＡＴＭ端末装置におけるグループ管理の負荷を低減できる。

【００６３】また、本実施例では、アドレス解決サーバ及び同報サーバは一対のものを用い、サーバと各ＡＴＭ端末装置、ブリッジとの間に確立されるコネクションの管理が容易になるので、ネットワーク側におけるアドレス解決サーバ及び同報サーバ等の資源を最小限にするとともに、効率の良いコネクションの確立と帯域利用を行うことができる。

【００６４】さらに、本実施例では、物理的に同一のＡＴＭ端末装置、ブリッジ間での通信であれば、単一のコネクションをシグナリング処理を用いて確立するだけで良く、通信は上記コネクション上のみで行われるので、従来の端末装置に特殊な処理を行わせることなく、既存端末装置との相互接続性を保つことができる。なお、本発明は、上記実施例に限らず、例えば支線ＬＡＮに接続されているＬＡＮ端末装置のアドレスについても、サーバの第１のアドレステーブルに登録させておくことも可能であり、この場合にはサーバがアドレス解決要求フレームをブリッジに転送する必要がなくなり、サーバにおいてネットワーク上の全端末のグループ管理が可能となる。

【００６５】また、本発明では、ブリッジの１つのポートに、複数のＶＬＡＮグループを重複して割り当てることも可能であり、また１つのポートに、複数の端末装置を接続させることも可能である。また、本実施例では、ＶＬＡＮ間は論理的に独立したものとなっているが、本発明はこれに限らず、特定のＶＬＡＮ間で通信を行うように設定することも可能である。

【００６６】

【発明の効果】以上説明したように、本発明では、第１端末装置がそれぞれ接続される複数のポートとブリッジ機能とを有する中継装置と、第２端末装置とを幹線ネットワークを介して直接接続させるとともに、前記中継装置の各ポート及び第２の端末装置をグループ分けして仮想ネットワークの設定を行い、送信元端末装置と通信許可された端末装置間でデータ通信を行うシステムにおいて、前記中継装置及び第２端末装置のアドレス情報と、該中継装置及び第２端末装置が属する少なくとも１つのグループ識別情報と、前記属するグループが少なくとも１つ異なる複数の第１端末装置が接続される中継装置であることを示すビット情報とを対応させて記憶する第１アドレス記憶部を有する記憶応答手段を、前記幹線ネットワークに接続させ、前記データ通信に先立って行われる宛先のネットワークアドレスの問い合わせに対して、前記記憶応答手段は、前記第１アドレス記憶部を検索して前記通信許可された端末装置間でのみデータ通信が行えるように、所定の応答を前記問い合わせを行った装置に返すので、複数のグループに属するブリッジ又はＡＴＭ端末装置におけるグループ管理の負荷を低減できるとともに、従来の端末装置に特殊な処理を行わせることなく、既存端末装置との相互接続性を保つことができる。

【００６７】請求項４では、前記第１アドレス記憶部に記憶されていない宛先のネットワークアドレスの問い合わせに対して、前記記憶応答手段は、該問い合わせを行った装置以外の中継装置及び第２端末装置に、該問い合わせを転送し、前記中継装置は、自装置に接続される第１端末装置のＭＡＣアドレスと、該各第１端末装置が属するグループ識別情報とを対応させて記憶する第２アドレス記憶部を有し、該第１端末装置のアドレスの問い合わせに対して、第２アドレス記憶部を検索し、該当アドレスに対応するグループ識別情報を含んだ所定応答を前記記憶応答手段に返すので、複数のグループに属するブリッジにおけるグループ管理の負荷を低減できる。

【００６８】請求項５では、前記問い合わせを行った中継装置は、前記記憶応答手段からの所定応答により得られた宛先のネットワークアドレスと、該宛先の属するグループ識別情報とを対応して記憶する第３アドレス記憶部を有し、自装置に接続された第１端末装置からの送信フレームの宛先に対して、該第３アドレス記憶部を検索し、宛先が属するグループと当該第１端末装置が属するグループ間で通信が許可されている場合のみ、該送信フレームを前記幹線ネットワークに送出するので、複数のグループに属するブリッジにおけるグループ管理の負荷を低減できる。

【００６９】請求項６，９では、前記記憶応答手段又は同報手段は、同報すべきフレームを受信した場合、前記第１アドレス記憶部の検索結果もしくは該同報フレームに付加されたグループ識別子より、送信元が属するグループを判断し、該送信元が属するグループ間で通信が許可されている場合のみ、該同報フレームを当該宛先に付加されたグループの中継装置又は第２の端末装置に転送するので、ネットワーク側におけるアドレス解決サーバ及び同報サーバ等の資源を最小限にするとともに、効率の良いコネクションの確立と帯域利用を行うことができる。

【００７０】請求項８，１２では、前記中継装置は、自装置に接続された第１端末装置からの同報フレームに対して、前記第２アドレス記憶部を検索し、該第１端末装置が属するグループ識別情報を付加した同報フレームを前記記憶応答手段に送出し、また該記憶応答手段から転送されてきた同報フレームに対しては、該同報フレームに付加されたグループ識別情報に基づいて、前記第２アドレス記憶部を検索し、該グループに属する第１の端末装置にのみ該同報フレームを中継するので、効率の良いコネクションの確立と帯域利用を行うことができる。

【図面の簡単な説明】

【図１】本発明に係る仮想ネットワーク管理方法を用いたバーチャルＬＡＮシステムの一実施例の構成を示す構成図である。

【図２】図１のシステムに用いられるフレームの構成を示すフレームフォーマットである。

【図３】図１に示したサーバのアドレス解決要求フレーム受信時の動作を説明するためのフローチャートである。

【図４】同じくサーバのアドレス解決応答フレーム受信時の動作を説明するためのフローチャートである。

【図５】同じくサーバの同報フレーム受信時の動作を説明するためのフローチャートである。

【符号の説明】

１０　ＡＴＭネットワーク

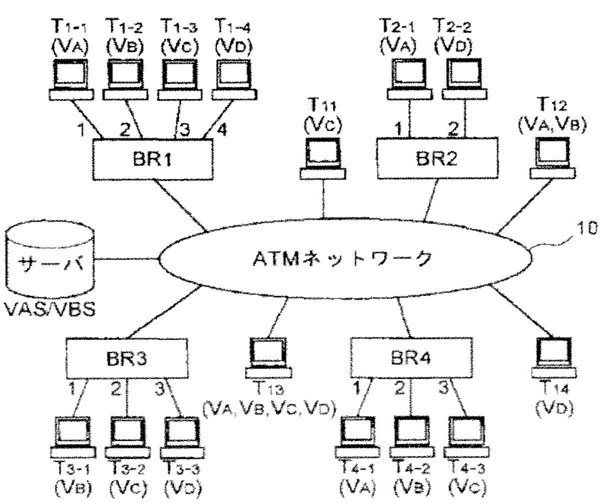
ＶＡＳ／ＡＢＳ　サーバ

ＢＲ1～ＢＲ4 ブリッジ

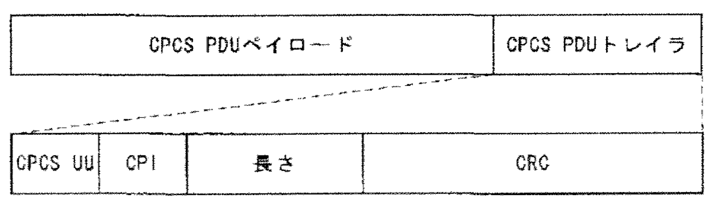
Ｔ11～Ｔ14　ＡＴＭ端末装置

Ｔ1-1～Ｔ1-4，Ｔ2-1，Ｔ2-2，Ｔ3-1～Ｔ3-3，Ｔ4-1～Ｔ4-3 ＬＡＮ端末装置

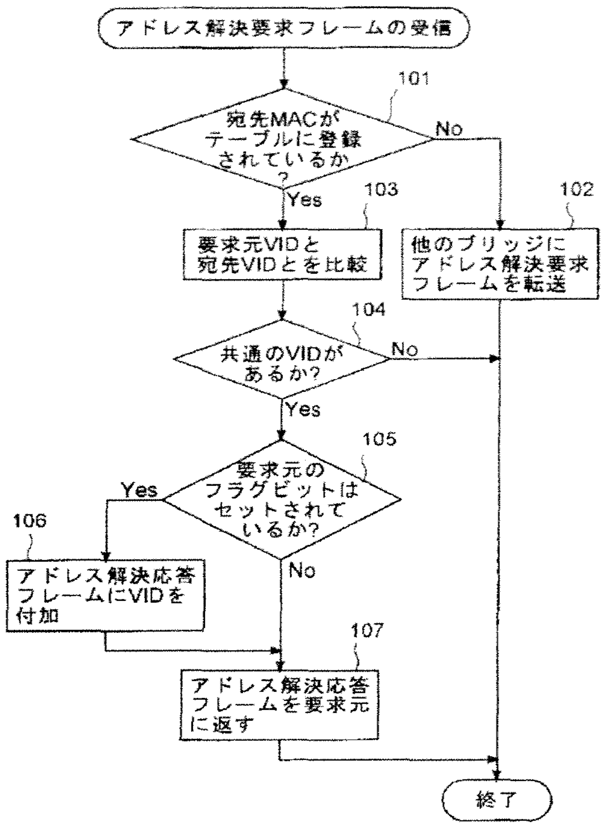
【図１】



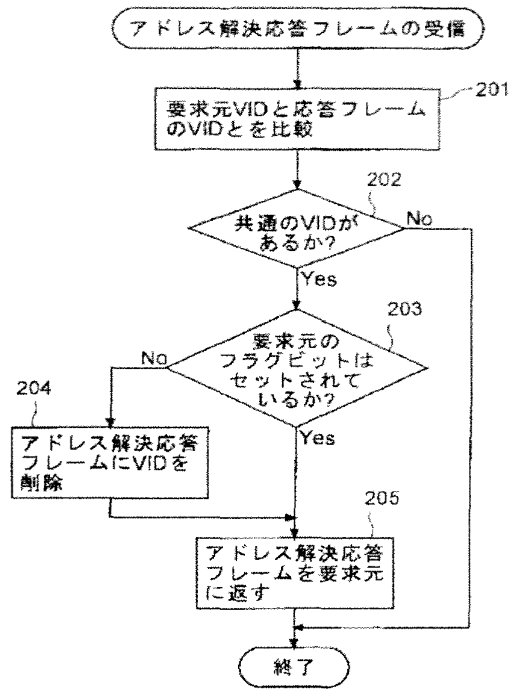
【図２】



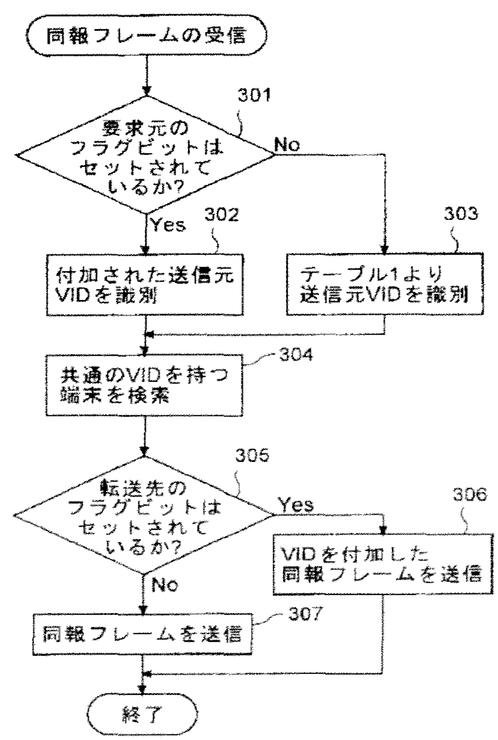
【図3】


アドレス解決要求フレームの受信
101
宛先MACがテーブルに登録されているか？
No
Yes
103
102
要求元VIDと宛先VIDとを比較
他のブリッジにアドレス解決要求フレームを転送
104
共通のVIDがあるか?
No
Yes
105
要求元のフラグビットはセットされているか?
Yes
106
No
アドレス解決応答フレームにVIDを付加
107
アドレス解決応答フレームを要求元に返す
終了

【図4】


アドレス解決応答フレームの受信
201
要求元VIDと応答フレームのVIDとを比較
202
共通のVIDがあるか?
No
Yes
203
要求元のフラグビットはセットされているか?
No
204
アドレス解決応答フレームにVIDを削除
Yes
205
アドレス解決応答フレームを要求元に返す
終了

【図5】


同報フレームの受信
301
要求元のフラグビットはセットされているか?
No
Yes
302
303
付加された送信元VIDを識別
テーブル1より送信元VIDを識別
304
共通のVIDを持つ端末を検索
305
転送先のフラグビットはセットされているか?
Yes
306
VIDを付加した同報フレームを送信
No
同報フレームを送信
307
終了

No documents available for this priority number.

Espacenet

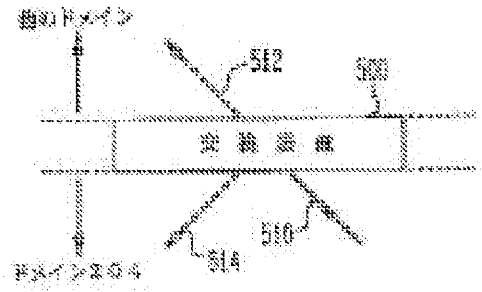
Bibliographic data: JP10111848 (A) — 1998-04-28

METHOD AND DEVICE FOR LIMITING ACCESS TO INDIVIDUAL INFORMATION OF DOMAIN NAME SYSTEM BY REDIRECTING ENQUIRY REQUEST

Inventor(s):	BELLOVIN STEVEN MICHAEL; CHESWICK WILLIAM ROBERT + (BELLOVIN STEVEN MICHAEL, ; CHESWICK WILLIAM ROBERT)
Applicant(s):	AT & T CORP + (AT & T CORP)
Classification:	**- international:** ***G06F13/00; H04L29/06; H04L29/12;*** (IPC1-7): G06F13/00; H04L12/28 **- cooperative:** H04L29/06; H04L29/12066; H04L29/12783; H04L61/1511; H04L61/35; H04L63/02
Application number:	JP19970189349 19970715
Priority number(s):	US19960679466 19960715
Also published as:	EP0825748 (A2) EP0825748 (A3) EP0825748 (B1) US5958052 (A) US5805820 (A) more

Abstract of JP10111848 (A)

PROBLEM TO BE SOLVED: To make it possible to limit access to individual information in the domain name system by redirecting all requests for domain names or IP addresses in a domain to another device, such as a domain name server, in the domain. SOLUTION: Illegal individual information is prevented from entering the domain. Here, a device in the domain is prevented from requesting individual information from a device outside the domain. Namely, a switching device 500 receives queries 510 of requests for domain name acquisition or address acquisition, searches for the contents of the respective requests, and redirects all the requests for the domain names or IP addresses of devices in the domain 204 as transfer requests 514 to the domain name server in the domain 204. The domain names of other devices outside the domain 204 to the domain server in the domain 204. The requests for the domain names or IP addresses of the devices outside the domain 204 are sent as forward requests 512 to a proper domain name server outside the domain 204.


512
510
514

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－111848

(43)公開日　平成10年(1998)４月28日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０６Ｆ　13/00	３５５	Ｇ０６Ｆ　13/00	３５５
	３５１		３５１Ｅ
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｚ

審査請求　未請求　請求項の数20　ＯＬ　（全 17 頁）

(21)出願番号　特願平9－189349

(22)出願日　平成９年(1997)７月15日

(31)優先権主張番号　０８／６７９４６６

(32)優先日　1996年７月15日

(33)優先権主張国　米国（ＵＳ）

特許法第65条の２第２項第４号の規定により図面第２，３，４，５，６，７，10，11図の一部は不掲載とする。

(71)出願人　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ＆Ｔ　ＣＯＲＰ．
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

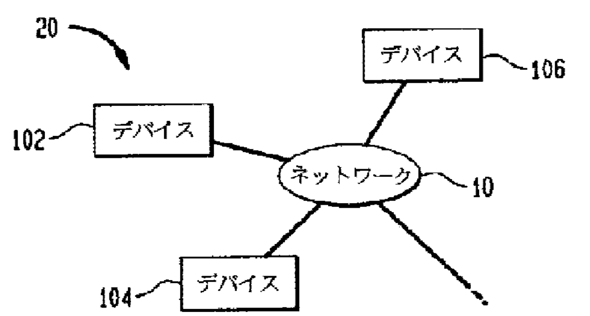
(72)発明者　スチーヴン　マイケル　ベロヴィン
アメリカ合衆国　07090　ニュージャーシィ，ウエストフィールド，キャッスルマン　ドライヴ　710

(74)代理人　弁理士　岡部　正夫　（外３名）

最終頁に続く

(54)【発明の名称】　照会要求を向けなおすことによってドメインネームシステムの個人情報へのアクセスを制限する方法と装置

(57)【要約】
【課題】　本発明は、ドメインネームシステムの個人情報へのアクセスの制限に関する。
【解決手段】　本発明は、第１のドメインの個人情報へのアクセスを制限するドメインネームシステムの下位システムであって、第１のドメインの第１のデバイスからの通信を受信する交換装置からなり、該通信は第２のドメインのデバイスに向けられた第１のドメインの個人情報に対する第１の要求を含み、該交換装置が個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおすことを特徴とする。



【特許請求の範囲】
【請求項１】　第１のドメインの個人情報へのアクセスを制限するドメインネームシステムの下位システムであって、該システムが、
第１のドメインの第１のデバイスからの通信を受信する交換装置からなり、該通信は第２のドメインのデバイスに向けられた第１のドメインの個人情報に対する第１の要求を含み、該交換装置が個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおすことを特徴とするシステム。
【請求項２】　請求項１に記載のシステムにおいて、通信が第１のドメインの個人情報でない情報に対する第２の要求を含み、交換装置が第２の要求を第２のドメインのデバイスに転送することを特徴とするシステム。
【請求項３】　請求項１に記載のシステムにおいて、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とするシステム。
【請求項４】　請求項１に記載のシステムにおいて、個人情報が、第１のドメイン中のデバイスのドメインネームと、第１のドメイン中のデバイスのＩＰアドレスの少なくとも１つを含むことを特徴とするシステム。
【請求項５】　請求項１に記載のシステムにおいて、第１のドメインが複数のデバイスからなり、該複数のデバイスが、第２のドメインとのすべての通信を交換装置に向けるように修正されることを特徴とするシステム。
【請求項６】　請求項１に記載のシステムにおいて、第１のデバイスがドメインネームサーバとレゾルバの１つであり、第１のデバイス以外の第１のドメイン中のデバイスから第１のデバイスに向けられる情報を要求することを特徴とするシステム。
【請求項７】　請求項１に記載のシステムにおいて、交換装置が第１のドメインのファイアウォールの一部分であることを特徴とするシステム。
【請求項８】　第２のドメインに接続された第１のドメインの個人情報へのアクセスを制限するためのドメインネームシステムの下位システムを操作する方法であって、該方法は、
第２のドメインのデバイスに向けられた、第１のドメインの第１のデバイスからの通信を受信する段階からなり、前記通信が第１のドメインの個人情報に対する第１の情報を含んでおり、該方法は更に、
第１のドメインの個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおす段階からなることを特徴とする方法。
【請求項９】　請求項８に記載の方法においてさらに、第１のデバイスからの通信の第２の要求を第２のドメインのデバイスに転送する段階からなり、該第２の要求は第１のドメインに個人的でない情報を要求することを特徴とする方法。
【請求項１０】　請求項８に記載の方法において、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とする方法。
【請求項１１】　請求項８に記載の方法において、個人情報が第１のドメインのドメインネームとＩＰアドレスの少なくとも１つであることを特徴とする方法。
【請求項１２】　ドメインネームシステムで使用する装置であって、該装置は、
第１のドメインの第１のデバイスからの通信を受信する交換装置からなり、前記通信は、第２のドメインのデバイスに向けられた第１のドメインの個人情報に対する第１の要求を含み、前記交換装置が個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおすことを特徴とする装置。
【請求項１３】　請求項１２に記載の装置において、通信は第１のドメインの個人情報でない情報に対する第２の要求を含み、交換装置が第２の要求を第２のドメインのデバイスに送ることを特徴とする方法。
【請求項１４】　請求項１２に記載の装置において、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とする装置。
【請求項１５】　請求項１２に記載の装置において、個人情報が第１のドメインのデバイスのドメインネームと第１のドメインのデバイスのＩＰアドレスの少なくとも１つであることを特徴とする装置。
【請求項１６】　請求項１２に記載の装置において、交換装置が第１のドメインのファイアウォールの一部分であることを特徴とする装置。
【請求項１７】　第２のドメインに接続された第１のドメインの個人情報へのアクセスを制限するための、ドメインネームシステムの装置を操作する方法であって、該方法が、
第２のドメイン中のデバイスに向けられる、第１のドメインの第１のデバイスからの通信を受信する段階からなり、前記通信が第１のドメインの個人情報に対する第１の要求を含んでおり、該方法は更に、
第１のドメインの個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおす段階からなることを特徴とする方法。
【請求項１８】　請求項１７に記載の方法においてさらに、
第１のデバイスからの通信の第２の要求を第２のドメインのデバイスに転送する段階をさらに含み、該第２の要求が第１のドメインに個人的でない情報を要求することを特徴とする方法。
【請求項１９】　請求項１７に記載の方法において、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とする方法。
【請求項２０】　請求項１７に記載の方法において、個人情報が、第１のドメインのドメインネームとＩＰアドレスの少なくとも１つであることを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の分野】本発明は、ドメインネームシステムの個人情報へのアクセスの制限に関する。

【0002】

【従来技術の説明】分散システムの多くは、ドメインネームとして知られる階層的な命名手法によって分散システムの名前を割り当てる。ドメインネームを使った分散システムはドメインネームシステム（ＤＮＳ）と呼ばれる。ドメインネームは点で区切られたドメインネームの連続である。例えば、research.att.comはドメインネームである。ｃｏｍは最上レベル・ドメインの最上レベル・ドメインネームであり、ａｔｔは第２レベル・ドメインの第２レベル・ドメインネームであり、ｒｅｓｅａｒｃｈは第３レベル・ドメインの第３レベル・ドメインネームである。あるドメイン中のデバイスは、ドメインネームを後に付けたデバイス名によって分類される。従って、research.att.comドメイン中の「server」と名付けられるデバイスは、server.research.att.com という名前を有する。デバイス名もまたドメインネームと呼ばれる。

【0003】ドメインネームは論理的かつ階層的な方法で分散システムを区分するが、メッセージはＩＰアドレスを使ってデバイスを識別することでＤＮＳのデバイス間を転送される。ＩＰアドレスは、191.192.193.2 のように、点で区切られた４つの８ビットの値によって表現される３２ビットの数字である。ＩＰアドレスには、デバイス・ネットワーク接続のネットワークＩＤおよびデバイスＩＤのような情報が含まれる。ＩＰアドレスはアドレス許可権限によって割り当てられる。アドレスは権限のあるアドレス・サーバにブロックで割り当てられる。

【0004】ＩＰアドレスはやはり階層的方法でお互いに関連するが、ドメインネーム階層とＩＰアドレス階層は直接お互いに関連しない。ドメインネームサーバにはアドレスサーバであるものもあるが、ドメインネームサーバとアドレスサーバが同じデバイスである必要はない。従って、あるサーバがドメインネームをデバイスの対応するＩＰアドレスに解決する権限を有しても、同じドメインネームサーバがＩＰアドレスを同じデバイスの対応するドメインネームに解決できないことがあり得る。従って、ＩＰアドレスのドメインネームへの解決には、異なったサーバが必要とされる以外は、ドメインネームのＩＰアドレスへの解決と同様の処理が続く。

【0005】ＩＰアドレスは数値で、ドメインネームとは異なってＤＮＳの論理的・階層的構成とは無関係に割り当てられるので、一般にデータ転送のような機能のための命令の際にはドメインネームが使われる。従って、データ転送命令はそのドメインネームによって受信装置を識別する。しかし、ドメインネームは、データ転送が行われる前に、対応するＩＰアドレスに変換しなければならない。

【0006】ドメインネームは、ドメインネームサーバと呼ばれる権限あるデバイスによって管理される。ドメインネームサーバはドメインネームを対応するＩＰアドレスに変換し、その逆の変換も行う。第１のデバイスが、ドメインネームだけがわかっている第２のデバイスにメッセージを転送したいと望む時、第１のデバイスはドメインネームサーバに照会して、第２のデバイスの既知のドメインネームに対応するＩＰアドレスを入手しなければならない。

【0007】ＩＰアドレス照会要求はかなり大きな分量になることがあり、ＤＮＳの効率を大きく低下させるので、ドメインネームサーバと関連するネットワークトラヒックの作業負荷を低減するために多くの手法が実行されてきた。しかし、これらの手法はＤＮＳの効率を改善したが、あるドメイン特定の個人の情報への無許可アクセスや、個人のマシンへのログインが可能になるなど、許可されない行為の機会を導入することにもなった。従って、ＤＮＳ内の個人情報へのアクセスを制限する必要がある。

【0008】

【発明の概要】侵入者はＤＮＳが使用するドメインネーム解決処理を利用することによってあるドメイン特定の個人の情報へのアクセスを得る。データ転送のような機能の命令は目的デバイスを指定するためにドメインネームを使用するので、ドメインネームは、データ転送が行われる前にＩＰアドレスに変換（解決（resolved、レゾルバ）しなければならない。侵入者はドメインネームをＩＰアドレスに解決するための処理を利用して個人情報へのアクセスを得るのである。詳細には、侵入者は不正なＩＰアドレスおよび／またはドメインネームを対象ドメインにパスし、正常なドメインネーム解決によって、目的デバイスの代わりに侵入者のデバイスのＩＰアドレスが作成されるようにする。

【0009】本発明は、ドメイン内のデバイスが、ドメイン外部のデバイスから個人情報を受け取る可能性をすべて除去することによって、侵入者がドメインの個人情報へのアクセスを得ることを防止する。詳細には、本発明は交換機能を行うＤＮＳプロキシデバイスを提供する。

【0010】交換機能はドメイン内のデバイスからドメインネームを解決するための照会要求を受信し、ドメイン内のデバイスのドメインネームまたはＩＰアドレスに対する要求をすべて、ドメインネームサーバのようなドメイン内の他のデバイスに向けなおす(redirect)。ドメインに個人的でない情報に対する要求はすべて、ドメイン外の目的デバイスに転送される。

【0011】詳細には、本発明は、第１のドメインの個人情報へのアクセスを制限するＤＮＳ内のシステムを提

供する。システムには交換装置が含まれる。交換装置は第１のドメインからの情報の要求をすべて受信し、個人情報に対する要求を第１のドメイン中の個人情報の権限ある情報源に向けなおす。第２のドメイン中のデバイスに向けられた、個人的でない情報に対する要求はすべて第２のドメイン中のデバイスに送られる。

【００１２】

【発明の詳細な記述】図1は、ネットワーク１０とデバイス１０２、１０４および１０６を含む分散システム２０の物理的接続を示す。分散システム２０は、図２に示すようなドメインネームシステム（ＤＮＳ）３０として構成される。

【００１３】ＤＮＳ３０は、ＤＮＳ３０中のドメインネームについて最高レベルの権限を保持するルート１００を有する。ルートは、それぞれ教育機関、会社機関、政府機関を表すｅｄｕ、ｃｏｍ、ｇｏｖといったドメインネームを割り当てる。これらの各ドメインはさらに、purdue.edu、att.com、nrl.govといった他のドメインに分割される。ルート１００は、ドメインネームに関する権限を、権限ドメインネームサーバと呼ばれる他のデバイスに委任する。例えば、ドメインatt.com はＡＴ＆Ｔ社が所有・管理している。ＡＴ＆Ｔ社はatt.com ドメイン内のドメインネームを割り当て・管理する権限を有する権限ドメインネームサーバとなるデバイスを指定する。従って、完全なＤＮＳ３０は複数のドメインに分割され、そこでは各ドメインの命名権限がそのドメインの権限ドメインネームサーバに帰属する。

【００１４】権限ドメインネームサーバはその命名権限を、そのドメイン内のまた別のサーバに委任する。例えば、att.com ドメインは、att.com 下のドメインネームに関する権限を有する権限ドメインネームサーバとしてserver.att.comという名称のデバイスを有する。att.comは、reserch.att.comと呼ばれる下位ドメインを有し、server.att.comは、reserch.att.com 下位ドメインに関する命名権限をserver.research.att.com と名付けられたデバイスに委任する。下位ドメインもドメインと呼ばれる。従って、server.research.att.com は、デバイス１０２に対するws1.reserach.att.comおよびデバイス１０４に対するws2.reserach.att.comのようなreserach.att.comドメイン中のデバイス名に関する命名権限を有する。

【００１５】server.buzbiz.com は、buzbiz.comドメインに関する権限ドメインネームサーバである。buzbiz.comドメインにはintru.buzbiz.comというドメインネームを有するデバイス１０６のようなデバイスが含まれる。

【００１６】図3は、ドメインpurdue.edu２０２、att.com２０４、buzbiz.com２０６、nrl.gov２０８およびルート２１０に分割されたＤＮＳ３０を示す。ルート・ドメイン１０１は、ドメインｅｄｕ、ｃｏｍおよびｇｏｖを含むことが示される。ドメインｅｄｕ、ｃｏｍおよびｇｏｖは、ルート・ドメインネームサーバ１００によって他の権限ドメインネームサーバに委任されるが、この場合、単一のドメインネームサーバであるルート１００は、ドメインｅｄｕ、ｃｏｍおよびｇｏｖに関する権限を維持している。

【００１７】前に論じたように、データはＩＰアドレスを使ってＤＮＳ３０中のデバイス１０２、１０４および１０６の間で転送される。図4は、デバイス１０２、１０４および１０６のＩＰアドレスを示す。データをデバイス１０６からデバイス１０２に転送するためには、デバイス１０６は目的ＩＰアドレスとして192.193.194.1を指定しなければならない。

【００１８】ＤＮＳ３０中の各デバイスは少なくとも１つのＩＰアドレスを有する。図5に示されるように、ドメイン２０４にはデバイス１０２、１０４、１０８および１１０が含まれる。上記の各デバイスはドメインネームとＩＰアドレスを有する。server.research.att.comは192.203.194.3というＩＰアドレスを有するデバイス１１０のドメインネームであり、server.research.att.comはresearch.att.comドメイン２１０に関する権限ドメインネームサーバである。research.att.comドメイン２１０にはそれぞれＩＰアドレス192.193.194.1と192.193.194.2を有するデバイス１０２と１０４が含まれる。

【００１９】ＤＮＳ３０中の各デバイスはドメインネームとＩＰアドレスを有するので、例えば、以下の表１と表２のような、２つの変換表が構成される。ドメインネームの表１は、各ドメインネームについて対応するＩＰアドレスを有し、ＩＰアドレスの表２は、各ＩＰアドレスについて対応するドメインネームを有する。表１がドメインネームによって整列され、表２がＩＰアドレスによって整列されれば、表１はドメインネームに対するＩＰアドレスを速やかに判定するのに使用され、表２はＩＰアドレスに対するドメインネームを速やかに判定するのに使用される。各ドメインネームサーバは、命名権限を有するすべてのデバイスに関する表１と表２に対応する表を含んでいる。権限ドメインネームサーバにはこの情報が含まれるので、他のデバイスは、権限ドメインネームサーバがその権限下にあるドメインネームのＩＰアドレスとＩＰアドレスのドメインネームをそれぞれ提供するように、アドレス獲得及びドメインネーム獲得要求を送信する。

【００２０】

【表１】

表 1

att. com	128. 129. 130. 1
research. att. com	192. 203. 194. 3
ws1. research. att. com	192. 193. 194. 1
ws2. research. att. com	192. 193. 194. 2

【表２】

表 2

128. 129. 130. 1	att. com
192. 193. 194. 1	ws1. research. att. com
192. 193. 194. 2	ws2. research. att. com
192. 203. 194. 3	research. att. com

【００２１】第１のデバイスは、ドメインネームで知られている第２のデバイスにデータを送信するという指示を受信すると、第２のデバイスのＩＰアドレスについて第２のデバイスの権限ドメインネームサーバに照会要求を送信する。権限ドメインネームサーバは要求された情報を返送するか、または命名権限が委任されているならば、権限ドメインネームサーバは、情報を有する別の権限ドメインネームサーバのドメインネームを返送する。ＩＰアドレスの獲得後、第１のデバイスはＩＰアドレスをデータを含むメッセージに組み込んで、メッセージを第２のデバイスに送信する。

【００２２】すべてのドメインネームサーバが命名権限を有するわけではない。ファイル・サーバに局所的であるデバイスが他のローカル・デバイスに容易にアクセスできるように、ファイル・サーバがドメインネームとＩＰアドレスを保留していることがある。こうしたファイル・サーバもまたドメインネームサーバまたは、ドメインネームをＩＰアドレスに解決し、またその逆の解決を行うためのレゾルバと呼ばれる。

【００２３】ドメインネームサーバ（権限のあるものとないもの）がそのドメインネームサーバの知らないＩＰアドレスを送る場合、そのＩＰアドレスは将来同じドメインネームを解決するためのリソース記録として、ドメインネームサーバのキャッシュ・メモリに保存される。従って、権限ドメインネームサーバもまた、ＩＰアドレスと対応するドメインネームを蓄積して、ドメインネームからＩＰアドレス、またその逆の有効な解決を促進する。従って、権限ドメインネームサーバは、ドメインネームを解決するためのレゾルバとも呼ばれる。

【００２４】ＤＮＳ３０の効率を改善しようとさらに努力して、ドメインネームサーバは、追加情報を照会要求の回答に添付することによって、他の関連デバイスのＩＰアドレスやドメインネームのような「追加情報」を伝えることが多い。レゾルバは将来アドレスを解決するために、追加情報を受信してキャッシュ・メモリに保存する。

【００２５】図6は、ドメイン２０４にはさらにレゾルバ１１２と１１４が含まれていることを示す。デバイス１０２と１０４は、それぞれ通信線３０２と３０８を経由して照会要求をレゾルバ１１２と１１４に送信し、ドメインネームをＩＰアドレスに解決する。レゾルバ１１２と１１４は、それぞれデバイス１０２と１０４に物理的に近接して位置している。例えば、レゾルバ１１２と１１４は、同じＬＡＮ上にあるか、または１つの建物内でデバイス１０２と１０４にそれぞれ近接して接続されている。従って、デバイス１０２と１０４が必要とするアドレスの解決は、ローカルＬＡＮ以外のネットワーク・トラヒックを一切使わずに行われる。

【００２６】しかし、レゾルバ１１２と１１４が、権限ある情報源から得たのではないＩＰアドレスを受信することによってドメインネームを解決する時、ＩＰアドレスは権限のないものとして照会デバイスに提供される。ＤＮＳ３０は一般にそれを速やかに変更しないので、多くの場合照会デバイスはとにかくそのＩＰアドレスを使用しようと判断する。

【００２７】ＤＮＳ３０は、例えば、機器が追加、移動または取り除かれると変更される。この動的な状況では、各リソース記録は、各リソース記録の寿命を示す寿命フィールド(time-to-live field)を含む。レゾルバ１１２と１１４は、リソース記録の寿命の値が終了すると、周期的にリソース記録を廃棄する。寿命の値は、ＩＰアドレスのようなリソース記録のコンテンツに対する権限を有するドメインネームサーバが設定する。

【００２８】前に論じたように、att.com はＡＴ＆Ｔ社が所有・管理するドメインである。従って、ＡＴ＆Ｔ社が管理するすべてのデバイスはatt.com ドメインの中にある。ＡＴ＆Ｔ社は、お互いに物理的に離れたサイトにatt.com ドメイン中のデバイスを分配する。例えば、デバイス１０２とレゾルバ１１２は１つのサイトに置かれ、デバイス１０４とレゾルバ１１４は別のサイトに置かれる。通信経路３０２、３０４及び３０８はatt.com ドメイン内のデバイス間の相互通信を表すが、通信経路３０４は地理的に離れた２地点間にある。通信経路３１０および３１２は、att.com ドメイン内のレゾルバ１１２および１１４と他のドメインのデバイスの間の通信経路を表す。

【００２９】att.com ドメイン内で交換される情報はＡＴ＆Ｔ社にとって貴重なものなので、att.com に個人的と思われる情報を無許可アクセスから保護することには重大な関心がある。ドメインの個人情報はそのドメインに関する何かを説明する情報である。個人情報を変更する権限はドメイン内にある。例えば、ＩＰアドレスとドメインネームはドメイン内の個人情報である。

【００３０】図7に示すように、ファイアウォール４０２のようなデバイスがドメイン２０４を出入りするデータ転送を制御するためにインストールされる。通信経路３１０および３１２は、通信線３１６を通じてドメイン２０４外のデバイスに達する前に、ファイアウォール４０２を通過する。ファイアウォール４０２はドメイン２０４からの個人情報の無許可転送を防止し、ドメイン２０４に個人的である情報に対するドメイン２０４外のデバイスからの要求を拒否する。

【００３１】しかし、従来のファイアウォールにはＤＮＳ３０のようなドメインネームシステムによって使われるドメインネーム解決方法を利用して間接的に得られる個人情報へのアクセスを防止できないものがある。詳細には、ドメインネームが対応するＩＰアドレスに解決される処理が、多数の方法の１つによって利用される。こうした方法のいくつかは以下の例で説明される。

【００３２】以下の例について、侵入者は対象デバイスと、自分が扮するユーザ名と、対象デバイスが委任するデバイスを確認しているので、委任されたデバイスが対象デバイスにログインする際パスワードは必要ないものと仮定する。侵入者はメール・メッセージまたはニュース記事から対象デバイスを識別する。対象デバイスが識別されると、侵入者は、簡易ネットワーク管理プロトコル（Simple NetworkManagement Protocol：ＳＮＭＰ）のような標準サービスを使って、対象デバイスを調査し、対象デバイスに接続された他のデバイスを発見する。さらに、「finger（フィンガ）」のようなサービスは、個人ユーザまたは他のユーザのシステムへのログオンに関する個人情報を提供する。さらに、メール・ヘッダには、明らかにメールの送り主であるファイル・サーバの名前と、通常ワークステーションの名前である、メールを出した実際のデバイスの名前が示されていることが多い。一般に、ファイル・サーバとそのファイル・サーバが取り扱うワークステーションはパスワードを使わずに通信する。従って、侵入者は標準的に利用可能なサービスを使って必要な情報をすべて得ることができる。

【００３３】侵入者が、buzbiz.comドメイン中のintru.buzbiz.comといった正当なドメインネームサーバを制御できると仮定すると、侵入者はintru.buzbiz.com内の任意のファイルを修正する能力を有する。侵入者がws1.reserach.att.comを対象として識別し、ws2.research.att.comをws1.research.att.comによって委任されたデバイスとして識別したならば、ＩＰアドレスを対応するドメインネームに変換するために使われる表２と同様の変換表を修正して、intru.buzbiz.comのＩＰアドレス（201.202.203.1） がドメインネームws2.research.att.comに対応するようにする。変換表の修正後、侵入者は、rlogin手続きを使用し、ws2.research.att.comのＩＰアドレスとして201.202.203.1を提供して、委任されたデバイスとしてws1.research.att.comへのログインを試みる。

【００３４】rlogin要求の受信後、ws1.research.att.comはＩＰアドレス201.202.203.1 についてドメインネーム獲得要求を実行し、対応するドメインネームを獲得する。intru.buzbiz.comはＩＰアドレス201.202.203.1 の権限あるアドレス・サーバであり、201.202.203.1 をその対応するドメインネームに変換する表を有しているので、ドメインネーム獲得要求は結局intru.buzbiz.comに送られる。しかし、その表はＩＰアドレス201.202.203.1 に対するドメインネーム獲得要求に対してintru.buzbiz.comの代わりにws2.research.att.comを出力するように変更されているので、ws2.research.att.comという間違ったドメインネームが返送される。従って、ws1.research.att.comは、ログイン要求に対応するデバイスのドメインネームとしてws2.research.att.comを受信する。ws2.research.att.comは委任された機器なので、ws1.research.att.comはログイン要求を受け入れ、侵入者がws1.research.att.comにログインするのを許可する。従って、侵入者がws1.research.att.com 内から到達可能なすべての個人情報へのアクセスを得る。

【００３５】個人情報への無許可アクセスを得るもう１つの方法はレゾルバ１１２のようなレゾルバのキャッシュ・メモリをだますことである。侵入者がws1.research.att.com を対象として識別したと仮定すると、侵入者は様々な方法でws1.research.att.comがintru.buzbiz.comに情報を照会するようにし向ける。ws1.research.att.com はレゾルバ１１２にアドレス獲得要求を送信して侵入者のデバイスintru.buzbiz.comのＩＰアドレスを獲得する。レゾルバ１１２はintru.buzbiz.comに関して何の情報も持っていないので、intru.buzbiz.comのドメインネームサーバに対してアドレス獲得要求を出力するが、それはこの場合intru.buzbiz.com自身である。intru.buzbiz.comは要求されたＩＰアドレスを返送するが、ws2.research.att.comのＩＰアドレスは正当なＩＰアドレス192.193.194.2 でなく、ＩＰアドレス201.202.203.1 に関連することを示す追加情報を添付する。侵入者は、自分の無許可アクセス完了直後にレゾルバ１１２が不正なリソース記録を消去するように、追加情報について非常に短い寿命を設定する。レゾルバはintru.buzbiz.comからの回答を受け入れ、前に論じたように、ws2.research.att.comに対する不正なＩＰアドレス201.202.203.1 と同様intru.buzbiz.comに対するＩＰアドレスを入力する。従って、レゾルバ１１２のキャッシュ・メモリはws2.research.att.comに対する不正なＩＰアドレスによってだまされる。

【００３６】次いで、intru.buzbiz.comは、201.202.203.1 をＩＰアドレスとして使ってws1.research.att.comにログインする。ws1.research.att.comがドメインネーム獲得指示を実行すると、レゾルバ１１２は、そのだまされたキャッシュの情報に基づいてws2.research.att.c omを返送する。するとws1.research.att.comは、ws2.research.att.comが委任されたデバイスなので、侵入者によるrlogin要求を承認する。その後、不正なＩＰアドレスのリソース記録の短い寿命が終了するので、レゾルバ１１２はリソース記録を破棄し、侵入の痕跡をすべて消去する。従って、侵入者は再びws1.research.att.com内からのすべての個人情報へのアクセスの獲得に成功する。

【００３７】侵入者は上記で論じたように、rlogin手続きの使用を制限されない。例えば、不正なＩＰアドレスがレゾルバ１１２またはws1.research.att.comによって一度受け入れられると、侵入者は、ws1.research.att.comによってws2.research.att.comに送信される任意のメッセージを傍受するよう選択できる。レゾルバ１１２は、ws1.research.att.comに、ws2.research.att.comのＩＰアドレスの代わりにintru.buzbiz.comに対応するＩＰアドレスを返送するので、傍受が可能である。ws2.research.att.comに向けられたws1.research.att.comの出力を受信した後、侵入者はデータをws2.research.att.comに送って、ws1.research.att.comとws2.research.att.comの間の通信が修正されずに続くようにする。従って、侵入者はパスワードのような個人情報を傍受でき、検出される機会は少ない。

【００３８】上記で説明した侵入者による個人情報への無許可アクセスが達成されるのは、ドメイン２０４内のデバイスがドメイン２０４外の信用できない情報源からドメイン２０４内の他のデバイスのＩＰアドレスを受信するからである。本発明は、以下で論じるように、２つの種類の通信が発生するのを防止することによって、ＩＰアドレスのような不正な個人情報がドメインに入ってくるのを防止する。

【００３９】１）本発明は、ドメイン内のデバイスが、ドメイン外のデバイスからの個人情報を要求することを防止する。図８に示すように、交換装置５００はドメインネーム獲得またはアドレス獲得要求の照会５１０を受信する。交換装置５００は各要求の内容を探索し、ドメイン２０４内のデバイスのドメインネームまたはＩＰアドレスに対する要求はすべて転送要求５１４としてドメイン２０４内のドメインネームサーバに向けなおされる。ドメイン２０４外のデバイスのドメインネームまたはＩＰアドレスに対する要求は順方向要求５１２としてドメイン２０４外の適当なドメインネームサーバに送られる。

【００４０】２）本発明は、個人情報がドメイン外部の信用できない情報源からドメイン内に入ってくるのを防止するフィルタ・デバイスを提供する。フィルタ・デバイスはドメイン外のデバイスが提供する個人情報をすべて排除する。

【００４１】図９に示されるように、フィルタ・デバイス５０２はドメイン２０４外部のデバイスからメッセージ５２０を受信する。フィルタ・デバイス５０２は、ＩＰアドレスやドメインネームのようなドメイン２０４に個人的である情報について受信されたメッセージ５２０を調査し、個人情報をメッセージから削除する。その後フィルタリングされたメッセージ５２２は、ドメイン２０４中の目的デバイスに送られる。

【００４２】図１０は、ドメイン２０４にＤＮＳプロキシ・デバイス４０４が含まれることを示す。ＤＮＳプロキシ４０４は、上記で説明した切り換え・フィルタリング機能を果たす。この実施形態では、ドメイン２０４内のデバイスは、すべての照会をＤＮＳプロキシ４０４に向けるように修正されている。ＤＮＳプロキシ４０４はドメイン２０４中のデバイスからのすべての照会要求を調査し、ドメイン２０４に個人的である情報に対する要求とそれ以外の情報に対する要求とを分離する。個人情報に対する要求は、server.att.comやserver.research.att.com のようなドメイン２０４内のドメインネームサーバに転送される。個人情報以外の情報に対する照会は、通信経路３２８を通じてファイアウォール４０２に送られ、次いでファイアウォールは、要求を通信経路３１６を通じて外部情報源に送る。

【００４３】図１０に示される実施形態は、照会要求をドメイン２０４外の適当なドメインネームサーバの代わりにＤＮＳプロキシ４０４に転送するレゾルバ１１２と１１４およびデバイス１１６のようなデバイスのソフトウェアの修正を必要とする。デバイス１１６はドメインネームサーバではなく、通信経路３２２を通じて直接外部情報源と通信する能力を有する。この実施形態では通信経路３１８、３２０および３２２は、ＤＮＳプロキシ４０４に転送される。

【００４４】通信経路３３０を通じて外部情報源から受信された情報はＤＮＳプロキシ４０４によってフィルタリングされる。ＤＮＳプロキシ４０４はドメイン２０４にはいるすべての情報を調査し、ドメイン２０４内のデバイスのＩＰアドレスのような、ドメイン２０４に個人的である情報をすべて排除する。外部情報源によって提供される情報に含まれる個人情報は、情報がドメイン２０４内の目的デバイスに送られる前に削除される。従って、照会要求に対する正当な回答に不正なＩＰアドレスを添付する試みはすべて排除される。

【００４５】通信経路３３０を通じて外部情報源から受信した情報も、ローカルセキュリティ保護管理ポリシーのために削除または修正される。例えば、外部情報源から受信した情報にドメイン２０４外のドメインネームサーバのポインタが含まれるならば、そのポインタは情報がドメイン２０４内の目的デバイスに送られる前に削除されなければならない。さもないと、ドメイン２０４内のデバイスが、こうしたドメインネームサーバにＤＮＳプロキシ４０４の介入なしに直接接触しようとすることがある。逆に、ドメイン２０４内のドメインネームサー

バのポインタが外部情報源から受信した情報に挿入されて、ドメイン２０４内の将来のドメインネームまたはアドレスの照会が直接、ＤＮＳプロキシ４０４の助けなしに解決されることがある。

【００４６】また、外部情報源から受信した電子メール交換記録のような情報が、ログ記録を保存するために、外向き電子メールをドメイン２０４内のログ・デバイス（図示せず）に転送するように修正されることがある。ログ記録はドメイン２０４内の個人情報の保護を支援する追加情報を提供する。

【００４７】図１１はＤＮＳプロキシ４０４がファイアウォール４０２に組み込まれることを示す。この実施形態では、ドメイン２０４内のデバイスのプログラムはどれも修正する必要はない。ドメイン２０４の個人情報の照会要求はすべて、通信経路３１０、３１２および３２２を通じて外部情報源に送られ続ける。しかし、ファイアウォール４０２内のＤＮＳプロキシは、ドメイン２０４の個人情報に対する照会要求をすべて、例えば、それぞれ通信経路３２４および３２６を通じてserver.att.comか、またはserver.research.att.com のどちらかに切り換える。通信経路３２２を通じて外部情報源から入力された情報は、フィルタリングされ、ドメイン２０４内の目的デバイスに送られる前に、すべての個人情報が削除される。

【００４８】図１２は、交換機能を行うＤＮＳプロキシ・サーバ４０４の処理を示す。ステップＳ１０００では、ＤＮＳプロキシ４０４は、ドメイン２０４外のデバイスに向けられた照会要求を受信し、ステップＳ１００２に進む。ステップＳ１００２では、ＤＮＳプロキシ４０４は各照会要求を調査し、個人情報がドメイン２０４外のデバイスから請求されているかを判断する。その後ＤＮＳプロキシ４０４はステップＳ１００４に進む。ステップＳ１００４では、ＤＮＳプロキシ４０４は、個人情報が要求されているならばステップＳ１００６に進む。さもなければ、ＤＮＳプロキシ４０４はステップＳ１０１０に進む。

【００４９】ステップＳ１００６では、ＤＮＳプロキシ４０４はドメイン２０４の個人情報に対する要求を、ドメイン２０４に個人的でない情報に対する要求から分離する。その後ＤＮＳプロキシ４０４はステップＳ１００８に進む。ステップＳ１００８では、ＤＮＳプロキシ４０４は、個人情報に対する要求をすべて、ドメイン２０４のドメインネームサーバのようなドメイン２０４内のデバイスに転送する。その後ＤＮＳプロキシはステップＳ１０１０に進む。

【００５０】ステップ１０１０では、ＤＮＳプロキシ４０４はドメイン２０４に個人的でない情報に対する要求をすべてドメイン２０４外のデバイスに送る。その後ＤＮＳプロキシ４０４はステップＳ１０１２に進み処理を終了する。

【００５１】図１３は、ドメイン２０４外のデバイスから受信した通信をフィルタリングするためのＤＮＳプロキシ４０４の処理を示す。ステップＳ２０００では、ＤＮＳプロキシ４０４は外部デバイスからの通信を受信してステップＳ２００２に進む。ステップＳ２００２では、ＤＮＳプロキシ４０４は個人情報に関する通信を調査してステップＳ２００４に進む。ステップＳ２００４では、ＤＮＳプロキシ４０４は、個人情報が外部デバイスからの通信中に発見されたならばステップＳ２００６に進み、さもなければＤＮＳプロキシ４０４はステップＳ２００８に進む。

【００５２】ステップＳ２００６では、ＤＮＳプロキシ４０４は通信からすべての個人情報を除去することによって通信をフィルタリングし、ステップＳ２００８に進む。ステップＳ２００８では、ＤＮＳプロキシ４０４はフィルタリングされた情報をドメイン２０４内の目的デバイスに送り、ステップＳ２０１０に進んで処理を終了する。

【００５３】本発明は特定の実施形態とともに説明されたが、多くの代替案、修正および別の形態が当業技術分野に熟練した者に明らかであることは明白である。従って、ここに示された本発明の好適実施形態は制限ではなく例示を目的としている。特許請求の範囲で示された本発明の精神と範囲から逸脱することなく、様々な変更が可能である。

【図面の簡単な説明】

【図１】図１は分散システムのブロック図である。

【図２】ドメインネームの階層を示す図である。

【図３】ドメインに分離された階層的ドメインネームの図である。

【図４】ＩＰアドレスを有するデバイスを伴う図３のドメインの図である。

【図５】対応するＩＰアドレスを伴うデバイスを有するドメインの図である。

【図６】お互いおよびドメイン外のデバイスと通信するデバイスを有する図５のドメインの図である。

【図７】ファイアウォールを有する図６に示されたドメインの図である。

【図８】交換装置の図である。

【図９】フィルタリング装置の図である。

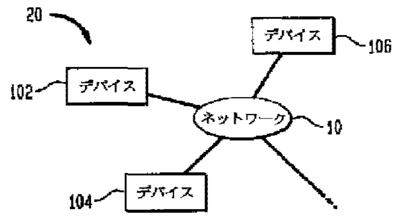
【図１０】ＤＮＳプロキシ・デバイスを含むドメインの図である。

【図１１】ファイアウォールに組み込まれたＤＮＳプロキシ・デバイスを含むドメインの図である。

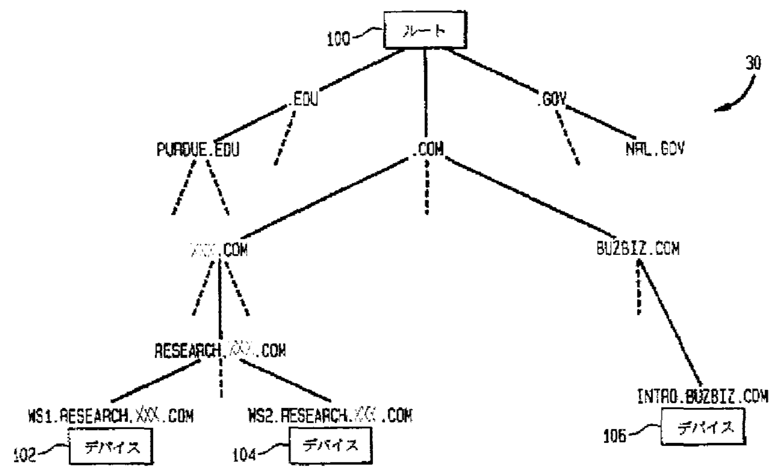
【図１２】交換装置の処理のフローチャートである。

【図１３】フィルタリング装置の処理のフローチャートである。

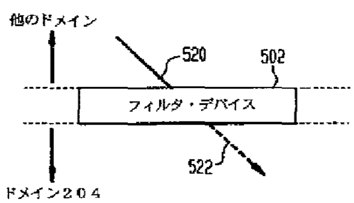
【図１】


20
デバイス
106
102
デバイス
ネットワーク
10
104
デバイス

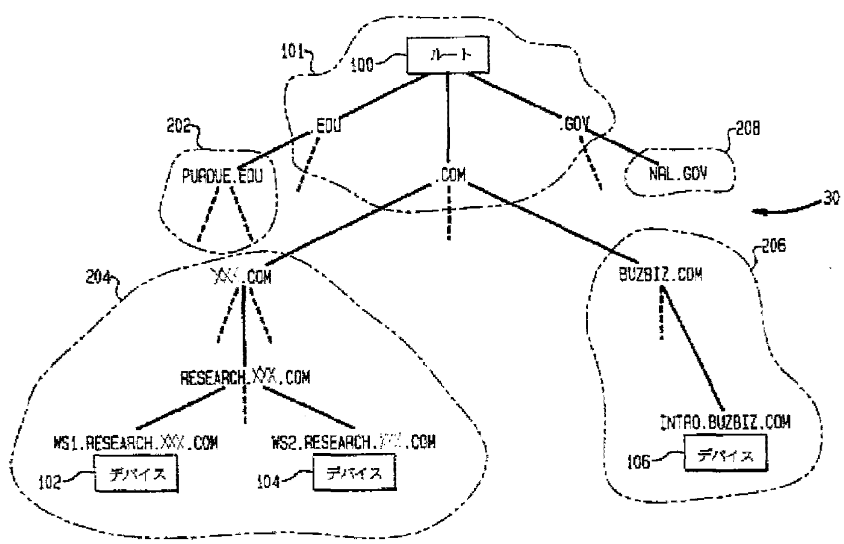
【図２】


100
ルート
30
.EDU
.GOV
PURDUE.EDU
.COM
NRL.GOV
BUZBIZ.COM
RESEARCH.
.COM
WS1.RESEARCH.XXX.COM
WS2.RESEARCH.
INTRO.BUZBIZ.COM
102
デバイス
104
デバイス
106
デバイス

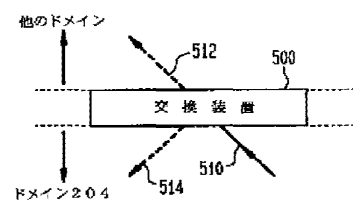
【図９】


他のドメイン
520
502
フィルタ・デバイス
522
ドメイン２０４

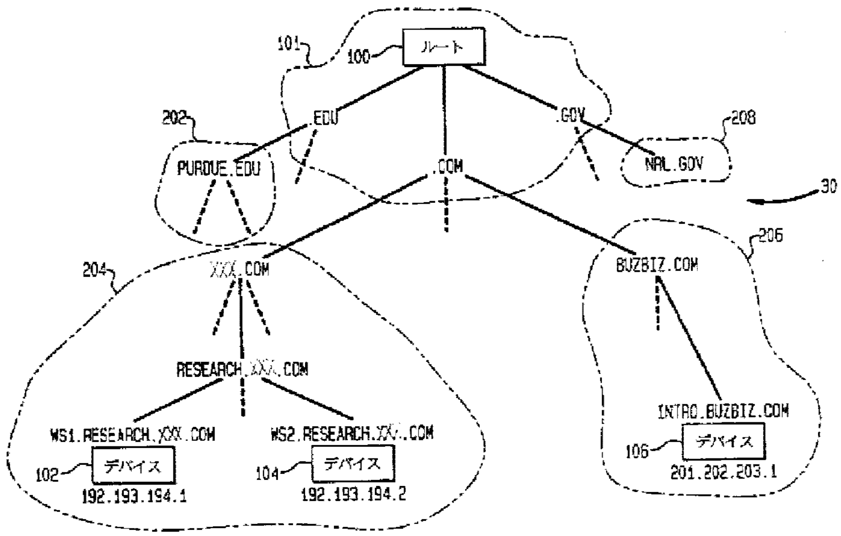
【図３】


101
100
ルート
202
.EDU
.GOV
208
PURDUE.EDU
.COM
NRL.GOV
30
206
204
.COM
BUZBIZ.COM
RESEARCH.XXX.COM
INTRO.BUZBIZ.COM
WS1.RESEARCH.XXX.COM
WS2.RESEARCH.
106
デバイス
102
デバイス
104
デバイス

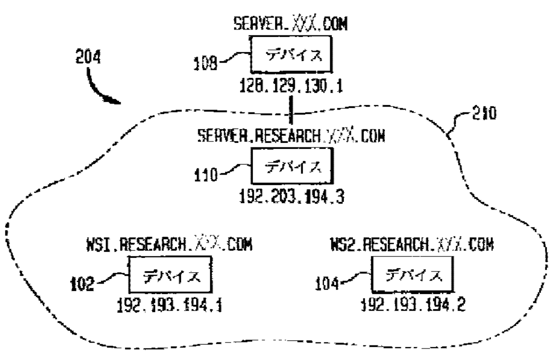
【図８】


他のドメイン
512
500
交換装置
510
514
ドメイン２０４

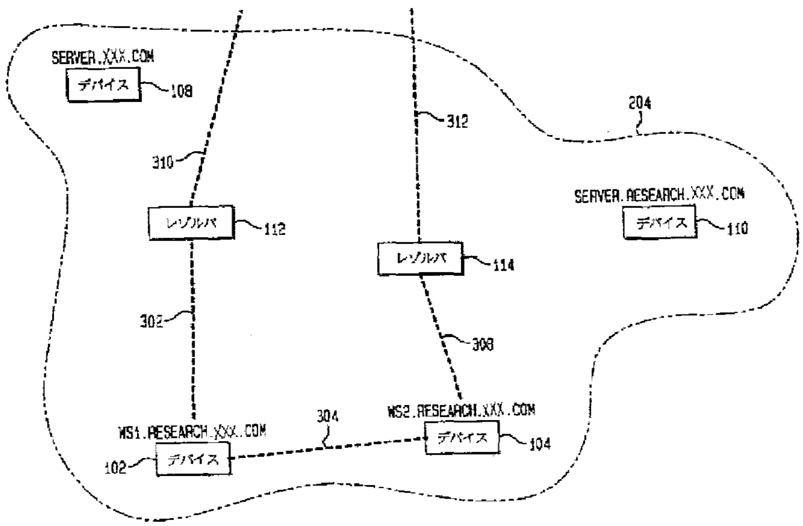
【図４】


ルート
100
101
.EDU
.GOV
.COM
202
PURDUE.EDU
208
NRL.GOV
30
204
XXX.COM
206
BUZBIZ.COM
RESEARCH.XXX.COM
WS1.RESEARCH.XXX.COM
WS2.RESEARCH.XXX.COM
デバイス
102
192.193.194.1
104
192.193.194.2
INTRO.BUZBIZ.COM
106
201.202.203.1

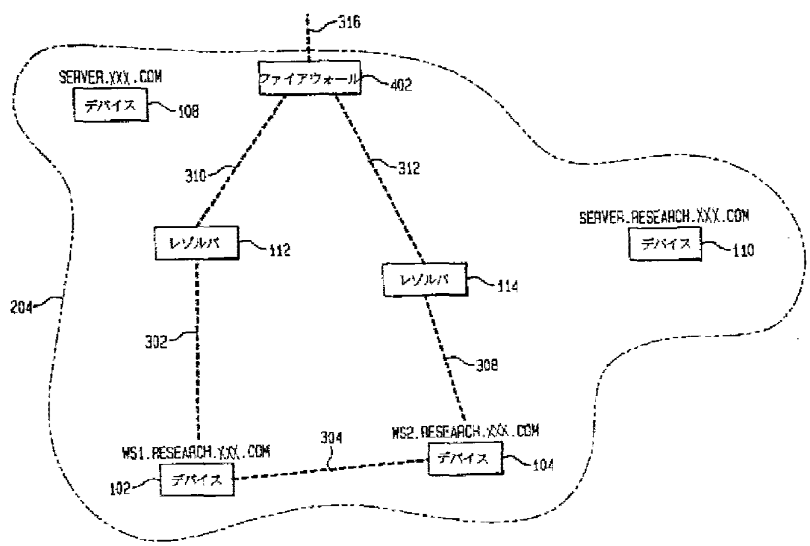
【図５】


SERVER.XXX.COM
204
108
デバイス
128.129.130.1
210
SERVER.RESEARCH.XXX.COM
110
192.203.194.3
WSI.RESEARCH.XXX.COM
WS2.RESEARCH.XXX.COM
102
192.193.194.1
104
192.193.194.2

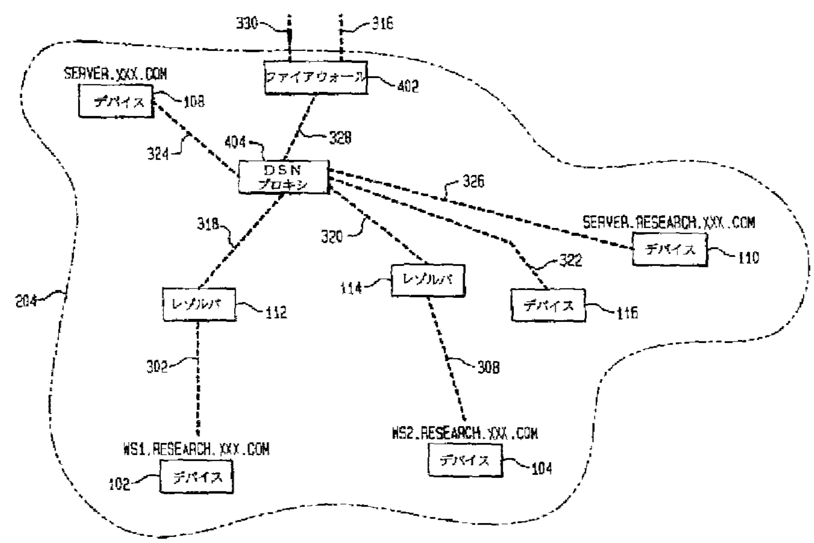
【図6】


SERVER.XXX.COM
デバイス
108
310
312
204
SERVER.RESEARCH.XXX.COM
デバイス
110
レゾルバ
112
レゾルバ
114
302
308
304
WS2.RESEARCH.XXX.COM
デバイス
104
WS1.RESEARCH.XXX.COM
102
デバイス

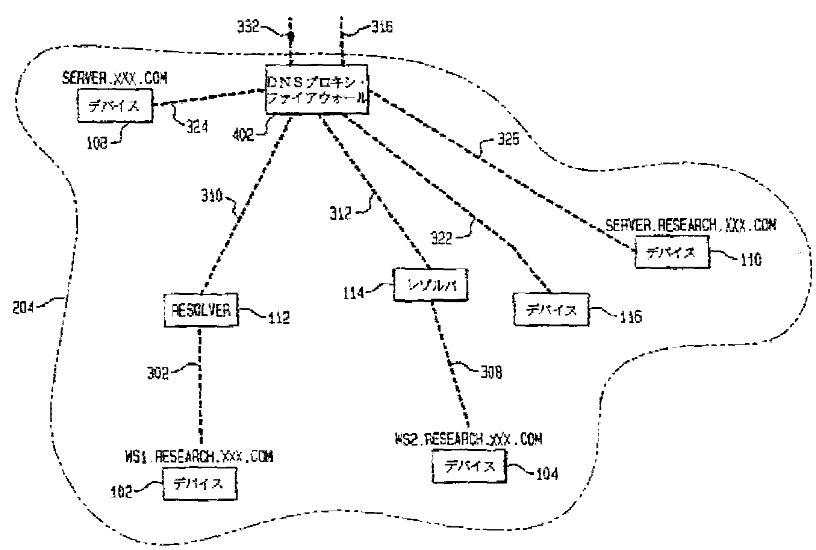
【図7】


316
ファイアウォール
402
SERVER.XXX.COM
デバイス
108
310
312
SERVER.RESEARCH.XXX.COM
デバイス
110
レゾルバ
112
レゾルバ
114
204
302
308
304
WS2.RESEARCH.XXX.COM
デバイス
104
WS1.RESEARCH.XXX.COM
102
デバイス

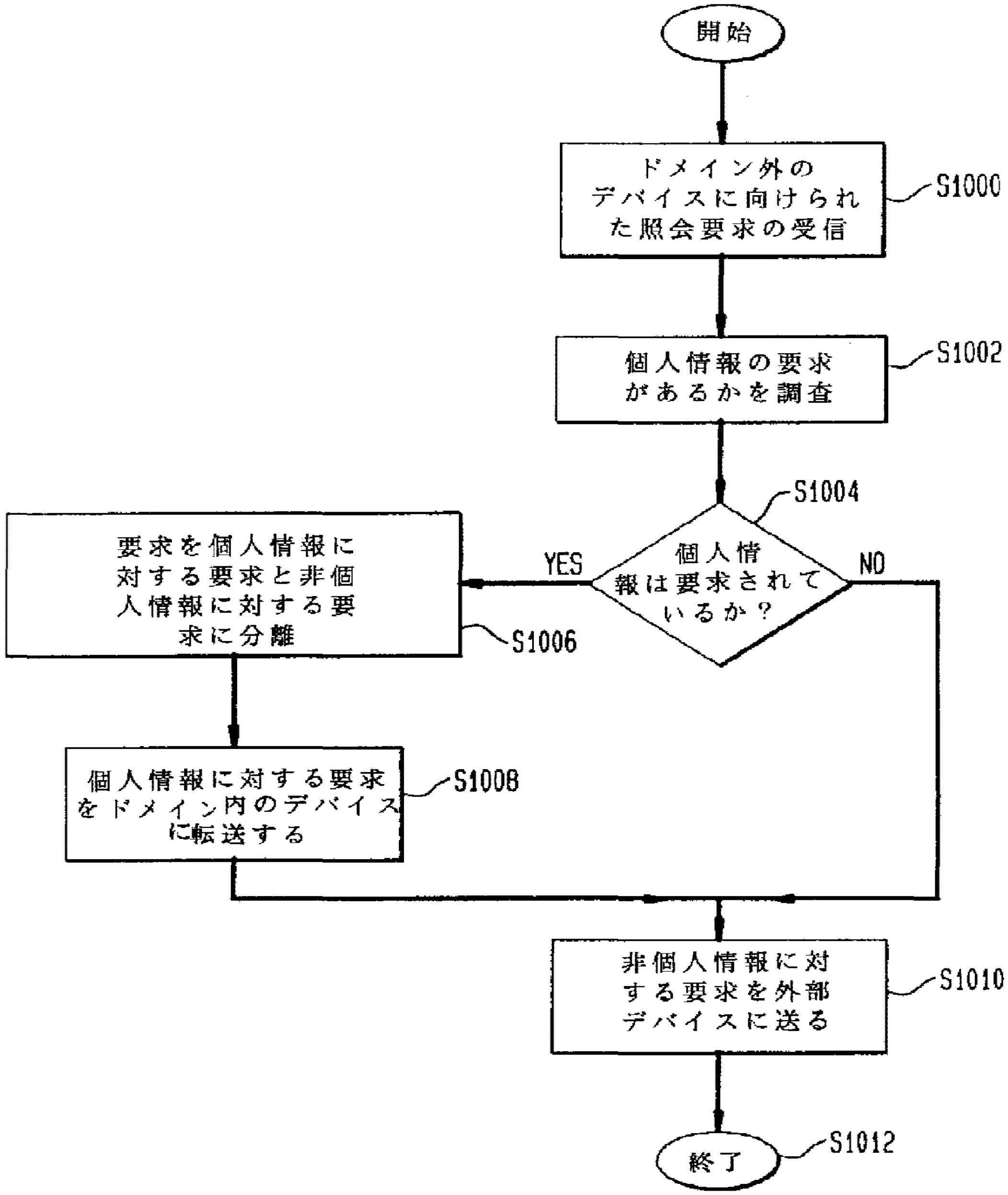
【図１０】


330
316
ファイアウォール
402
SERVER.XXX.COM
デバイス
108
404
328
324
DSN
プロキシ
326
SERVER.RESEARCH.XXX.COM
デバイス
110
318
320
322
114
レゾルバ
デバイス
116
204
レゾルバ
112
302
308
WS2.RESEARCH.XXX.COM
デバイス
104
WS1.RESEARCH.XXX.COM
102
デバイス

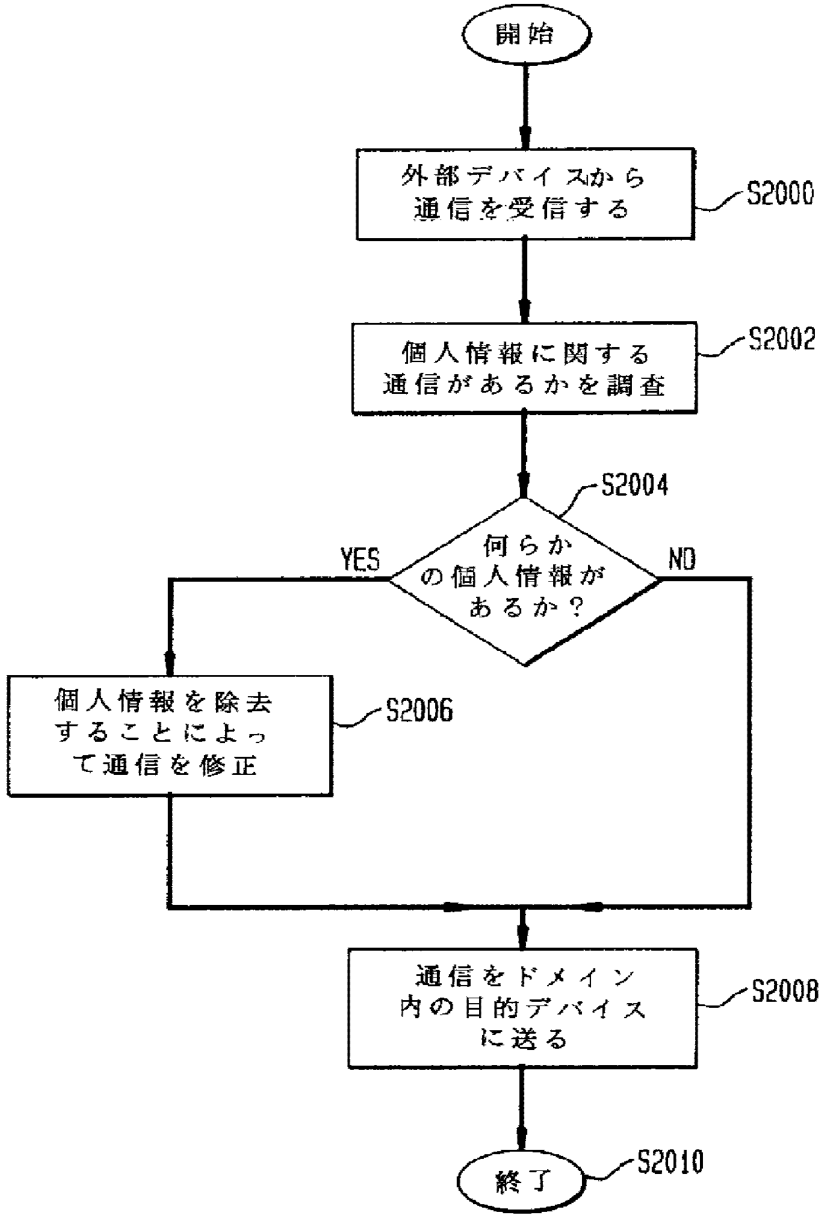
【図１１】


332
316
SERVER.XXX.COM
DNSプロキシ・
ファイアウォール
デバイス
324
108
402
326
310
312
322
SERVER.RESEARCH.XXX.COM
デバイス
110
114
レゾルバ
204
RESOLVER
112
デバイス
116
302
308
WS2.RESEARCH.XXX.COM
デバイス
104
WS1.RESEARCH.XXX.COM
102
デバイス

【図12】


開始
ドメイン外の
デバイスに向けられ
た照会要求の受信
S1000
個人情報の要求
があるかを調査
S1002
S1004
個人情
報は要求されて
いるか？
YES
NO
要求を個人情報に
対する要求と非個
人情報に対する要
求に分離
S1006
個人情報に対する要求
をドメイン内のデバイス
に転送する
S1008
非個人情報に対
する要求を外部
デバイスに送る
S1010
終了
S1012

【図13】



【手続補正書】
【提出日】平成９年１２月１０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】　第１のドメインの個人情報へのアクセスを制限するドメインネームシステムの下位システムであって、該システムが、
第１のドメインの第１のデバイスからの通信を受信する交換装置からなり、該通信は第２のドメインのデバイスに向けられた第１のドメインの個人情報に対する第１の要求を含み、該交換装置が個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおすことを特徴とするシステム。
【請求項２】　請求項１に記載のシステムにおいて、通信が第１のドメインの個人情報でない情報に対する第２

の要求を含み、交換装置が第２の要求を第２のドメインのデバイスに転送することを特徴とするシステム。
【請求項３】　請求項１に記載のシステムにおいて、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とするシステム。
【請求項４】　請求項１に記載のシステムにおいて、個人情報が、第１のドメイン中のデバイスのドメインネームと、第１のドメイン中のデバイスのＩＰアドレスの少なくとも１つを含むことを特徴とするシステム。
【請求項５】　請求項１に記載のシステムにおいて、第１のドメインが複数のデバイスからなり、該複数のデバイスが、第２のドメインとのすべての通信を交換装置に向けるように修正されることを特徴とするシステム。
【請求項６】　請求項１に記載のシステムにおいて、第１のデバイスがドメインネームサーバとレゾルバの１つであり、第１のデバイス以外の第１のドメイン中のデバイスから第１のデバイスに向けられる情報を要求することを特徴とするシステム。
【請求項７】　請求項１に記載のシステムにおいて、交換装置が第１のドメインのファイアウォールの一部分であることを特徴とするシステム。
【請求項８】　第２のドメインに接続された第１のドメインの個人情報へのアクセスを制限するためのドメインネームシステムの下位システムを操作する方法であって、該方法は、
第２のドメインのデバイスに向けられた、第１のドメインの第１のデバイスからの通信を受信する段階からなり、前記通信が第１のドメインの個人情報に対する第１の情報を含んでおり、該方法は更に、
第１のドメインの個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおす段階からなることを特徴とする方法。
【請求項９】　請求項８に記載の方法においてさらに、第１のデバイスからの通信の第２の要求を第２のドメインのデバイスに転送する段階からなり、該第２の要求は第１のドメインに個人的でない情報を要求することを特徴とする方法。
【請求項１０】　請求項８に記載の方法において、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とする方法。
【請求項１１】　請求項８に記載の方法において、個人情報が第１のドメインのドメインネームとＩＰアドレスの少なくとも１つであることを特徴とする方法。
【請求項１２】　ドメインネームシステムで使用する装置であって、該装置は、
第１のドメインの第１のデバイスからの通信を受信する交換装置からなり、前記通信は、第２のドメインのデバイスに向けられた第１のドメインの個人情報に対する第１の要求を含み、前記交換装置が個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおすことを特徴とする装置。
【請求項１３】　請求項１２に記載の装置において、通信は第１のドメインの個人情報でない情報に対する第２の要求を含み、交換装置が第２の要求を第２のドメインのデバイスに送ることを特徴とする方法。
【請求項１４】　請求項１２に記載の装置において、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とする装置。
【請求項１５】　請求項１２に記載の装置において、個人情報が第１のドメインのデバイスのドメインネームと第１のドメインのデバイスのＩＰアドレスの少なくとも１つであることを特徴とする装置。
【請求項１６】　請求項１２に記載の装置において、交換装置が第１のドメインのファイアウォールの一部分であることを特徴とする装置。
【請求項１７】　第２のドメインに接続された第１のドメインの個人情報へのアクセスを制限するための、ドメインネームシステムの装置を操作する方法であって、該方法が、
第２のドメイン中のデバイスに向けられる、第１のドメインの第１のデバイスからの通信を受信する段階からなり、前記通信が第１のドメインの個人情報に対する第１の要求を含んでおり、該方法は更に、
第１のドメインの個人情報に対する第１の要求を第１のドメインの第２のデバイスに向けなおす段階からなることを特徴とする方法。
【請求項１８】　請求項１７に記載の方法においてさらに、
第１のデバイスからの通信の第２の要求を第２のドメインのデバイスに転送する段階をさらに含み、該第２の要求が第１のドメインに個人的でない情報を要求することを特徴とする方法。
【請求項１９】　請求項１７に記載の方法において、第２のデバイスが第１のドメインのドメインネームサーバであることを特徴とする方法。
【請求項２０】　請求項１７に記載の方法において、個人情報が、第１のドメインのドメインネームとＩＰアドレスの少なくとも１つであることを特徴とする方法。
【請求項２１】　情報をフィルタリングするドメインネームシステムの下位システムであって、該下位システムが、
第２ドメインの第２デバイスに向けられた第１ドメインの第１デバイスからの情報を受信するフィルタリング装置からなり、該フィルタリング装置が、情報から第２ドメインの個人情報を除去し、フィルタリングされた情報を第２ドメインの第２デバイスに転送することによって、フィルタリングされた情報を生成することを特徴とするシステム。
【請求項２２】　請求項２１に記載のシステムにおいて、第２ドメインの個人情報が第２ドメインのデバイス

のドメインネームとＩＰアドレスの少なくとも１つを含むことを特徴とするシステム。

【請求項２３】　請求項２１に記載のシステムにおいて、情報が第２ドメインの第２デバイスによる照会要求に応答して第１ドメインの第１デバイスによって送信され、該情報が第２ドメインの第２デバイスによって要求されていない追加情報を含み、フィルタリング装置が第２ドメインの第２デバイスによって要求されていない追加情報から第２ドメインの個人情報を除去することを特徴とするシステム。

【請求項２４】　請求項２１に記載のシステムにおいて、フィルタリング装置がローカル機密保護管理ポリシーに基づいて情報を修正することによってフィルタリングされた情報を生成することを特徴とするシステム。

【請求項２５】　請求項２４に記載のシステムにおいて、ローカル機密保護管理ポリシーが、デバイスのポインタを伴う第１のドメインの第１のデバイスから受信された情報から第１のドメインのデバイスへポインタを置換するか、第１ドメインの第１デバイスから受信したメール交換記録を修正かの、少なくともいずれか１つであることを特徴とするシステム。

【請求項２６】　情報をフィルタリングするドメインネームシステムの下位システムを操作する方法であって、該方法が、

第２ドメインの第２デバイスに向けられた第１ドメインの第１デバイスから情報を受信する段階と、

第１デバイスから受信された情報から第２ドメインの個人情報を除去することによってフィルタリングされた情報を生成する段階と、

フィルタリングされた情報を第２ドメインの第２デバイスに転送する段階からなることを特徴とする方法。

【請求項２７】　請求項２６に記載の方法において、第２デバイスの個人情報は、第２ドメインのデバイスのドメインネームとＩＰアドレスの少なくとも１つを含むことを特徴とする方法。

【請求項２８】　請求項２６に記載の方法において、情報が、第２ドメインの第２デバイスによる照会要求に反応して第１ドメインの第１デバイスによって送信され、該情報が、第２ドメインの第２デバイスによって要求されない追加情報を含み、フィルタリングされた情報を生成する段階が、

第２ドメインの第２デバイスによって要求されない追加情報から第２ドメインの個人情報を除去する段階からなることを特徴とする方法。

【請求項２９】　請求項２６に記載の方法においてさらに、ローカル機密保護管理ポリシーに基づいて、情報を修正する段階からなることを特徴とする方法。

【請求項３０】　請求項２１に記載の方法において、ローカル機密保護管理ポリシーは、デバイスのポインタを伴う第１のドメインの第１のデバイスから受信された情報から第１のドメインのデバイスへポインタを置換するか、第１ドメインの第１デバイスから受信したメール交換記録を修正かの、少なくともいずれか１つであることを特徴とする方法。

【請求項３１】　ドメインネームシステムで使用する装置であって、該装置は、

第２ドメインの第２デバイスに向けられた第１ドメインの第１デバイスからの情報を受信するフィルタリング装置からなり、該フィルタリング装置は、情報から第２ドメインの個人情報を除去し、そしてフィルタリングされた情報を第２ドメインの第２デバイスに転送することによってフィルタリングされた情報を生成することを特徴とする装置。

【請求項３２】　請求項３２に記載の装置において、第２ドメインの個人情報が、第２ドメインのデバイスのドメインネームとＩＰアドレスの少なくとも１つを含むことを特徴とする装置。

【請求項３３】　請求項３１に記載の装置において、情報は、第２ドメインの第２デバイスによる照会要求に応答して第１ドメインの第１デバイスによって送信され、該情報が第２ドメインの第２デバイスによって要求されない追加情報を含み、該フィルタリング装置が第２ドメインの第２デバイスによって要求されない追加情報から第２ドメインの個人情報を除去することを特徴とする装置。

【請求項３４】　請求項３１に記載の装置において、フィルタリング装置がローカル機密保護管理ポリシーに基づいて情報を修正することによってフィルタリングされた情報を生成する装置。

【請求項３５】　請求項３４に記載の装置において、ローカル機密保護管理ポリシーが、デバイスのポインタを伴う第１のドメインの第１のデバイスから受信された情報から第１のドメインのデバイスへポインタを置換するか、第１ドメインの第１デバイスから受信したメール交換記録を修正かの、少なくともいずれか１つであることを特徴とする装置。

【請求項３６】　情報をフィルタリングするドメインネームシステムの装置を操作する方法であって、該方法は、

第２ドメインの第２デバイスに向けられた、第１ドメインの第１デバイスからの情報を受信する段階と、

第１デバイスから受信された情報から第２ドメインの個人情報を除去することによってフィルタリングされた情報を生成する段階と、

フィルタリングされた情報を第２ドメインの第２デバイスに転送する段階からなることを特徴とする方法。

【請求項３７】　請求項３６に記載の方法において、第２ドメインの個人情報が第２ドメインのデバイスのドメインネームとＩＰアドレスの少なくとも１つを含むことを特徴とする方法。

【請求項３８】　請求項３６に記載の方法において、情報は第２ドメインの第２デバイスによる照会要求に応答して、第１ドメインの第１デバイスによって送信され、該情報が第２ドメインの第２デバイスによって要求されない追加情報を含み、フィルタリングされた情報を生成する段階が、
第２ドメインの第２デバイスによって要求されない追加情報から第２ドメインの個人情報を除去する段階からなることを特徴とする方法。
【請求項３９】　請求項３６に記載の方法においてさらに、ローカル機密保護管理ポリシーに基づいて情報を修正する段階からなることを特徴とする方法。
【請求項４０】　請求項３９に記載の方法において、ローカル機密保護管理ポリシーが、デバイスのポインタを伴う第１のドメインの第１のデバイスから受信された情報から第１のドメインのデバイスへポインタを置換するか、第１ドメインの第１デバイスから受信したメール交換記録を修正かの、少なくともいずれか１つであることを特徴とする装置。

フロントページの続き

(72)発明者　ウイリアム　ロバーツ　チェスウィック
アメリカ合衆国　07924　ニュージャーシィ，バーナーズヴィル，マイン　マウント　ロード　93

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-215244**

(43)Date of publication of application : **11.08.1998**

(51)Int.Cl. **H04L 9/14**

H04L 9/36

(21)Application number : **09-012810**

(22)Date of filing : **27.01.1997**

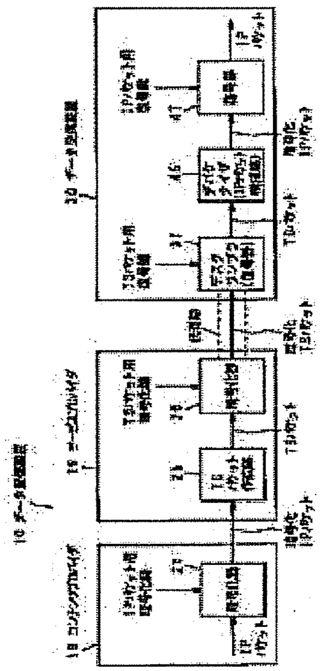
(71)Applicant : **SONY CORP**

(72)Inventor : **KUBOTA ICHIRO**
ASANO TOMOYUKI

(30)Priority

Priority number : **08316726** Priority date : **27.11.1996** Priority country : **JP**

(54) **INFORMATION TRANSMITTER AND METHOD, INFORMATION RECEIVER AND METHOD, AND INFORMATION STORAGE MEDIUM**



(57)Abstract:

PROBLEM TO BE SOLVED: To provide the information storage medium that stores digital data received through a data transmission channel from an information server together with a contents ID depending on a type of the data.

SOLUTION: A data distributer 10 applies duplicate encryption processing to digital data together with encryption processing using a cryptographic key depending on an identifier denoting a kind of the digital data and transmits the duplicate encryption data to a data receiver 30. The data receiver 30 receives the duplicate encryption data sent from the data distributer 10 through a satellite channel and applies decoding processing to the data by using respective decoding keys corresponding to the respective encryption keys.

CLAIMS

[Claim(s)]
[Claim 1]In information transmission equipment which divides digital data into a predetermined data block, and transmits this data block via a data transmission line, Information transmission equipment comprising:
A transmitting means which performs at least two-fold encryption processing, and transmits this encoded data including encryption processing using an encryption key according to an identifier which shows a kind of the above-mentioned digital data to the above-mentioned digital data.
A receiving means which receives the above-mentioned encoded data transmitted via a written data transmission line from the above-mentioned transmitting means, and performs decoding processing using each decode key according to each encryption key.

[Claim 2]The information transmission equipment according to claim 1, wherein the above-mentioned predetermined data block is a packet by Internet Protocol for transmitting and receiving digital data via a network between two or more systems.
[Claim 3]The information transmission equipment according to claim 1 before the above-mentioned receiving means's decrypting all the received above-mentioned encoded data, wherein it saves written data temporarily at a memory measure.
[Claim 4]The information transmission equipment according to claim 1 characterized by having a bidirectional data transmission line in which bidirectional data communications are possible separately from a written data transmission line.
[Claim 5]The information transmission equipment according to claim 4 characterized by using a terrestrial communication network as the above-mentioned bidirectional data transmission line using satellite connection with larger transmission capacity than the above-mentioned bidirectional data transmission line as a written data transmission line.
[Claim 6]In an information transmission method which divides digital data into a predetermined data block, and transmits this data block via a data transmission line, Encryption processing using an encryption key according to an identifier which shows a kind of the above-mentioned digital data to the above-mentioned digital data is included, An information transmission method performing decoding processing to the above-mentioned encoded data which transmitted this encoded data after performing at least two-fold encryption processing, and was received via a written data transmission line using each decode key according to each encryption key.
[Claim 7]The information transmission method according to claim 6, wherein the above-mentioned predetermined data block is Paquette by Internet Protocol for transmitting and receiving digital data via a network between two or more systems.
[Claim 8]The information transmission method according to claim 6 characterized by saving written data temporarily at a storage medium before decrypting all the received above-mentioned encoded data.
[Claim 9]The information transmission method according to claim 6 characterized by having a bidirectional data transmission line in which bidirectional data

communications are possible separately from a written data transmission line.
[Claim 10]The information transmission method according to claim 9 characterized by using a terrestrial communication network as the above-mentioned bidirectional data transmission line using satellite connection with larger transmission capacity than the above-mentioned bidirectional data transmission line as a written data transmission line.
[Claim 11]An information storage medium with which encryption processing using an encryption key according to an identifier which shows a kind of digital data is characterized by having memorized encoded data given at least.
[Claim 12]Information reception equipment extracting and decoding only a data block of a kind which read the above-mentioned identifier and was previously registered in information reception equipment which receives multiplexing data which consists of two or more kinds of data blocks to which an identifier which shows a kind of data was added via a data transmission line.
[Claim 13]The information reception equipment according to claim 12 having an identifier of a data block of a receivable kind in a reference table with the identifier and a corresponding decode key.
[Claim 14]The information reception equipment according to claim 13 characterized by performing decoding processing to this encryption data block based on a decode key according to an identifier with reference to the above-mentioned reference table when the enciphered above-mentioned data block is received.
[Claim 15]The information reception equipment according to claim 12 using Paquette by Internet Protocol for transmitting and receiving digital data via a network between two or more systems as the above-mentioned data block.
[Claim 16]The information reception equipment according to claim 12 using a transmission destination address included in a header of the Internet protocol packet for transmitting and receiving digital data via a network between two or more systems as the above-mentioned identifier.
[Claim 17]The information reception equipment according to claim 12 using content ID showing a kind of information on the above-mentioned data block as the above-mentioned identifier.
[Claim 18]The information reception equipment according to claim 12 having the above-mentioned identifier in a media-access-control header to which it was added by head of each data block.
[Claim 19]The information reception equipment according to claim 18 having Flagg for expressing classification of the above-mentioned identifier in the above-mentioned media-access-control header added to a head of each above-mentioned data block.
[Claim 20]The information reception equipment according to claim 12 characterized by having a bidirectional data transmission line in which bidirectional data communications are possible separately from a written data transmission line.
[Claim 21]The information reception equipment according to claim 12 characterized by using a terrestrial communication network as the above-mentioned bidirectional data transmission line using satellite connection with larger transmission capacity than the above-mentioned bidirectional data transmission line as a written data transmission line.
[Claim 22]An information receiving method extracting and decoding only a data block of a kind which read the above-mentioned identifier and was previously registered in an information receiving method which receives multiplexing data which consists of two or more kinds of data blocks to which an identifier which shows a kind of data was added via a data transmission line.
[Claim 23]The information receiving method according to claim 22 having an identifier of a data block of a receivable kind in a reference table with the identifier and a corresponding decode key.
[Claim 24]The information receiving method according to claim 23 characterized by performing decoding processing to this encryption data block based on a decode key according to an identifier with reference to the above-mentioned reference table when

the enciphered above-mentioned data block is received.
[Claim 25]The information receiving method according to claim 22 using a packet by Internet Protocol for transmitting and receiving digital data via a network between two or more systems as the above-mentioned data block.
[Claim 26]The information receiving method according to claim 22 using a transmission destination address included in a header of the above-mentioned Internet protocol packet as the above-mentioned identifier.
[Claim 27]The information receiving method according to claim 22 using content ID showing a kind of information on the above-mentioned data block as the above-mentioned identifier.
[Claim 28]The information receiving method according to claim 22 having the above-mentioned identifier in a header of media access control to which it was added by head of each data block.
[Claim 29]The information receiving method according to claim 28 having Flagg for expressing classification of the above-mentioned identifier in the above-mentioned media-access-control header added to a head of each above-mentioned data block.
[Claim 30]The information receiving method according to claim 22 characterized by using a bidirectional data transmission line in which bidirectional data communications are possible separately from a written data transmission line.
[Claim 31]The information receiving method according to claim 30 characterized by using a terrestrial communication network as the above-mentioned bidirectional data transmission line using satellite connection with larger transmission capacity than the above-mentioned bidirectional data transmission line as a written data transmission line.
[Claim 32]An information storage medium memorizing two or more kinds of data blocks to which content ID which shows a kind of information on a data block was added.
[Claim 33]The information storage medium according to claim 32, wherein the above-mentioned content ID is distinguished by a flag in a media-access-control header added to a head of each data block.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]The present invention relates to the information transmission equipment, the method, the information reception equipment, method, and information storage medium for offering data distribution service, for example using a communications satellite.
[0002]
[Description of the Prior Art]When [which carries out data communications using a dial-up line a dedicated line, etc.] case or talking over the telephone, in order to prevent leakage of transmitted data, or in order to maintain the reliability of information to the disturbance over transmitted data, the data of the plaintext was enciphered and transmitted and the data enciphered in the reception destination is decoded.
[0003]As a typical cipher system, the common key encryption system and the public-key crypto system are known. The common key encryption system is also called the symmetrical cryptosystem, and there are an algorithm nondisclosure type and an algorithm public presentation type. DES (Date Encryption Standard) is known as a typical algorithm public presentation type thing. Since computational complexity immense in order to derive a decode key from an enciphering key is required and a decode key is not decoded substantially, a public-key crypto system is a cipher system which may exhibit an enciphering key.
It is also called an unsymmetrical key cipher system.

[0004]Fig.17 is a schematic structure figure showing an example of the encoded data transmission equipment which enciphers the data on a transmission line with a common key encryption system. This encoded data transmission equipment protects that the bugging device 93 by the side of a tapping person intercepts data from the data transmission line 94 which connects the sending set 91 by the side of a sending person, and the receiving set 92 by the side of an addressee.
[0005]Encryption processing which uses the encryption key 97 with the encryption machine 96 in the sending set 91 is performed to the data which should be transmitted. The above-mentioned encoded data which was transmitted by the data transmission line 94 and received with the receiving set 92 is decoded by the decoder 99 which used the decode key 98, and decode data is obtained.
[0006]Since it does not have the decode key 98 even if the bugging device 93 receives here the data similarly enciphered as the receiving set 92 from the data transmission line 94, it is difficult to decode. That is, in the bugging device 93, since the data which required then incomprehensible encryption processing (scramble) as it is will be treated, it can prevent leaking information to the bugging device 93 side actually. Generally in the main encryption methods of the common key encryption system in this example, an enciphering key and a decode key are identical-bits sequences.
[0007]A cipher system which was mentioned above is determined according to the classification of the circuit system to which transmission data is transmitted, the degree of secrecy (confidentiality) of transmission data, the quantity of transmission data, etc. For example, in the data communications using a dedicated line, although leakage of information and the degree of the disturbance to transmission data are low, when carrying out data communications using a dial-up line, the degree of leakage of information and the degree of disturbance become high.
[0008]
[Problem to be solved by the invention]By by the way, the thing for which transmission of the digital data using a communications satellite was attained in recent years, Although transmitted [came] using the communications satellite also about the text, and the digital video and voice data which are used not only by analog video and voice data, such as television broadcasting and a movie, but by computer etc., Since reception with many and unspecified receiving sets is possible, the degree of leakage of information and the degree of disturbance become still higher.
[0009]That is, in the data transmission system using the above-mentioned communications satellite, since many and unspecified addressees can receive easily with a receiving set unlike 1 to 1 communication of a telephone line, a dedicated line, etc., it is easy to be intercepted. For this reason, a possibility that charged data communications will be intercepted, for example is high. Then, a data encryption is needed also a written data transmission system.
[0010]In a actual written data transmission system, encryption processing is performed about not all data, Using the information which the data which should be enciphered was enciphered according to the contents of the data which should be transmitted in a sending set, it sent out on the transmission line, and the addressee decoded all or some of enciphered data, and was acquired as a result, Or it is got to know whether the data is required for itself by the portion transmitted without being enciphered.
[0011]Here, the conventional television broadcast service using a communications satellite is a form as for which a many user uses the data which the distribution person distributed receiving it simultaneously. On the other hand, when distributing the digital data used by computer etc. via a communications satellite, the function which distributes data to the specific user of the singular number or plurality from a data distribution person is called for.
[0012]However, conventionally, in the simultaneous transmissive communication or broadcasting system from a data distribution person to many users, All Users received the always same information, use or an inspection was carried out, and since there was

no identification information of a system user individual, distribution of data only to a specific user from a data distribution person was not completed.
[0013]The present invention is made in view of the above-mentioned actual condition, and also when it transmits digital data using the above-mentioned communications satellite, it aims at offer of the information transmission equipment and the method of making the degree of leakage of information, and the degree of disturbance low.
[0014]The present invention is made in view of the above-mentioned actual condition, and aims at offer of the information reception equipment and the method only a specific user enables it to receive the digital data transmitted via the data transmission line from the information distributor according to the kind of data.
[0015]The present invention is made in view of the above-mentioned actual condition, and aims at offer of the information storage medium which has memorized the enciphered encoded data with the encryption key according to the identifier of the digital data by the transmitting information person side at least.
[0016]The present invention is made in view of the above-mentioned actual condition, and aims at offer of the information storage medium which has memorized the digital data transmitted via the data transmission line from the information distributor with the content ID according to the kind of data.
[0017]
[Means for solving problem]In order that the information transmission equipment and the method concerning the present invention may solve an aforementioned problem, After performing at least two-fold encryption processing including the encryption processing using the encryption key according to the identifier which shows the kind of the above-mentioned digital data to the above-mentioned digital data, this encoded data is transmitted, Decoding processing is performed to the above-mentioned encoded data received via the data transmission line using each decode key according to each encryption key.
[0018]In order that the information storage medium concerning the present invention may solve an aforementioned problem, the encryption processing by the encryption key according to the identifier which shows the kind of digital data has memorized the encoded data given at least.
[0019]In order to solve an aforementioned problem, the information reception equipment and the method concerning the present invention receive two or more kinds of data blocks to which the identifier which shows the kind of data was added via a data transmission line, read the above-mentioned identifier, and extract and decode only the data block of the kind registered previously.
[0020]The information storage medium concerning the present invention memorizes two or more kinds of data blocks to which the content ID which shows the kind of information on a data block was added, in order to solve an aforementioned problem.
[0021]
[Mode for carrying out the invention]It describes referring to Drawings for the embodiment of the information transmission equipment concerning the present invention, a method, information reception equipment, a method, and an information storage medium hereafter. This embodiment is a data transmission system of the Fig.1 which divides digital data into a predetermined data block, and transmits this data block via satellite connection.
[0022]This data transmission system is provided with the following.
The data distribution device 10 which performs double encryption processing and transmits this duplicate encryption data including encryption processing using an encryption key according to an identifier which shows a kind of the above-mentioned digital data to digital data.
The data receiver 30 which receives the above-mentioned duplicate encryption data transmitted via the above-mentioned satellite connection from this data distribution device 10, and performs decoding processing using each decode key according to each

encryption key.
Here, the expansion slot of a personal computer is equipped with the data receiver 30, for example. The personal computer is shown in Fig.1 as the data receiver 30 as it is.
[0023]The data distribution device 10 and the data receiver 30 can communicate mutually via a terrestrial communication network like ISDN in which bidirectional communication is possible. This terrestrial communication network may be connected to the Internet which transmits and receives digital data via a network between two or more systems. The satellite connection by the communications satellite 18 has transmission capacity larger than the above-mentioned terrestrial communication network.
[0024]First, the data flow in a written data transmission system is described. Here, it is assumed that the specific user who owns the data receiver 30 with the data donor who owns the data distribution device 10 has made the contract of delivery of data previously. With the data donor here, both the entrepreneur (henceforth a content provider) who provides transmitted data, and the entrepreneur (henceforth a service provider) who provides a transmission line are included.
[0025]The user who owns the data receiver 30 sends the request of the purport that he would like to receive the predetermined service which a data donor provides to the data distribution device 10, for example via ISDN as a terrestrial communication network. The method in particular of sending this request may not be limited, but may be decided by the kind of data, or a contract state with a user, for example, mail etc. may be sufficient as it. In accordance with a contract, a data donor may provide service previously, without sending a request.
[0026]The request from a user sent to the data distribution device 10 is received by the data request reception part 11, and is sent to the data management part 12. The data management part 12 will perform the read request of data to the data accumulation part 13, if the contract information and the request of a user check that it is that meaningful and it is satisfactory. The data accumulation part 13 sends data to the data creation part 15 via the high-speed switcher 14, according to a data read demand for example.
[0027]In the data creation part 15, to the data from the data accumulation part 13, IP-packet-izing, Format conversion, such as formation of a media-access-control (Media Access Control, MAC) frame and transport-izing of MPEG(Moving Picture Experts Group Phase) 2, is performed. The data creation part 15 enciphers the above-mentioned duplex after IP-packet-izing of data, and transport-izing.
[0028]It describes below about this format conversion. As mentioned above, it becomes possible for various kinds of data like an audio, a video signal, or data to multiplex, and to be transmitted by a mass digital circuit in recent years. As the method of this multiplexing, the transport stream (Transport Stream, TS) packet which is a transmission format of MPEG 2, for example is known. In this TS packet, encryption processing has been performed to the information data part (payload part). The peculiar bit string corresponding to 13 bits packet ID (PID) of the header part of a TS packet and a 2-bit scramble control part is used for the enciphering key for this encryption. Above-mentioned PID is used to identify information kinds, such as video of the specific channel of each TS packet, and an audio.
[0029]In transmitting data using this TS packet, data is converted to the format of the Internet Protocol (IP) packet currently widely used on the Internet, and it puts this IP packet into a TS packet further.
[0030]By the way, when various kinds of data is transmitted as an IP packet, it is used in order that above-mentioned PID may discriminate the data of an IP packet from other videos or the data of an audio, Bit length is also the number of bits insufficient for making the classification of various data which has only 13 bits and is transmitted by an IP packet identify. Then, the identifying method of kinds of data other than PID is needed.
[0031]For example, on the Internet, the transmission destination address

(DestinationAddress) included in identifying whether received data are data addressed to themselves at the IP header of an IP packet is used. Even when transmitting an IP packet by a TS packet, it is possible to identify whether it is data addressed to itself using this transmission destination address (it is henceforth called a transmission destination IP address.).

[0032]However, it is dramatically difficult for a data transmission rate to serve as 30Mbps per one translator, if satellite connection is taken for an example, for example, and to analyze a transmission destination IP address by software in real time by a data receiving side. By a certain means, a means to extract only the information addressed to oneself is needed.

[0033]It is very convenient, if only the information on the genre of its interested information is specified even if it does not specify the title of specific information, and only the information on the genre is received automatically and can download.

[0034]When data is enciphered as having mentioned above in order to consider it as ability ready for receiving only at a specific member, it is necessary to decode the enciphered data in a receiving side.

[0035]So, in the written data transmission system, added the identifier which shows the kind of data to the multiplexing data which consists of two or more kinds of data blocks in the data distribution device 10, and it was made to go via the communications satellite 18, and has transmitted to the data receiver 30 by the above-mentioned satellite connection. And in the data receiver 30, the above-mentioned identifier is read in hardware, and only the data of the classification registered previously which an addressee needs is extracted and decoded.

[0036]Addition of this identifier is performed by the data creation part 15 of the data distribution device 10. It is accumulated in the data accumulation part 13 in the data distribution device 10 in the state where no data which a user needs is processed. From the data management part 12, the data accumulation part 13 told that the read request of data came from the user sends the destination information of the requested data and a user to the data creation part 15 via the high-speed switcher 14 simultaneously.

[0037]Here, a user's destination information is a transmission destination IP address required for IP packet transmission. In this data transmission system, the transmission destination IP address peculiar to all the users is assigned. While the user of 1 has secured the transmission destination IP address which the user of 1 has, no users other than the user of one have.

[0038]Creation or after format conversion is carried out, the data from the data accumulation part 13 is multiplexed with other audio signals and a video signal by the data processing part 16, and is sent to the communications satellite 18 by the data creation part 15 via a wireless circuit from the transmission antenna 17 as multiplexing data.

[0039]The multiplexing data sent via the communications satellite 18 can be received by all the users who are in the situation where not only the data receiver 30 that a specific user owns but data is receivable. The data receiver 30 receives all the multiplexing data from the communications satellite 18, and sorts out, extracts and decrypts the data according to the request which he advanced from the inside.

[0040]This data receiver 30 extracts and decodes only the data block of the kind registered previously by receiving the multiplexing data which consists of two or more kinds of data blocks to which the identifier which shows the kind of data was added via the satellite connection by the communications satellite 18, and reading the above-mentioned identifier.

[0041]Namely, the data receiver 30 receives the many data block containing the data transmitted according to the request, sorts out the data block addressed to itself, the data block which he should receive, and the data block which he can receive, and extracts it from the inside. The data receiver 30 which a user has is previously determined by the contract of a user and a data donor.

[0042]Therefore, if it is usual, the characteristic data of other addressing to a user cannot be sorted out using the data receiver 30 which a user has.
[0043]However, in the written data transmission system using the communications satellite 18, since many and unspecified addressees can receive easily with a receiving set unlike 1 to 1 communication of a telephone line, a dedicated line, etc., it is easy to be intercepted. That is, a possibility that data communications will be intercepted is high. Then, a data encryption is needed also a written data transmission system.
[0044]For this reason, the data distribution device 10 is with contents propa- Ida 18 who provides information, and service propa- Ida 19 who transmits that information, and has performed double encryption processing with the encryption machine 21 and the encryption machine 26 so that it may be shown briefly [Fig.2].
[0045]Actually, this data distribution device 10 is constituted, as shown in the Fig.1 mentioned above, and each part which the content provider 18 who showed especially Fig.2, and service propa- Ida 19 have is contained in the data creation part 15 as shown in Fig.3.
[0046]The data and the IP address addressed to a specific user which have been sent from the data accumulation part 13 are sent to the transmission destination IP packet preparing part 20. In the IP packet preparing part 20, IP packet 60 shown in Fig.4 is generated using the data sent from the data accumulation part 13, and the transmission destination IP address which specifies a user at the time. The size of this IP packet 60 is prescribed by TCP/IP (Transmission Control Protocol/Internet Protocol), When the data which the user requested exceeds that size, this data is divided into two or more IP packets, and is transmitted to the following encryption machine 21.
[0047]Transmission destination IP address 74 of the user who shows Fig.5, and IP address 73 of the transmitting agency are contained in the IP header of IP packet 60 used here. Here, transmission destination IP address 74 is 32 bits.
[0048]IP packet 60 created by the IP packet preparing part 20 is transmitted to the encryption machine 21. In the encryption machine 21, the IP packet 60 whole is enciphered with the enciphering key for IP packets which an address gets to know that he is a specific user, and already gets to know mutually only at Hazama, a data donor and a specific user, at the time by 32-bit above-mentioned transmission destination IP address 74 in IP packet 60. As an encryption expression, DES (Data Encryption Standard) etc. are adopted, for example.
[0049]the limited reception by encryption of an IP packet since this encryption machine 21 performs encryption which used 32 above-mentioned bits transmission destination IP address 74 -- an addressee can be divided into the range of the 32nd power (= about 4,300 millions) individual of 2.
[0050]Here, the content provider 18 gives previously the transmission destination IP address of the IP packet to transmit, and the decode key for decoding an encryption IP packet to the data receiver 30. And the payload part of an IP packet is enciphered with the encryption key corresponding to this decode key, and it sends to the service provider 19.
[0051]However, the encryption needs to give about no data to a specific user, and encryption may not be performed depending on the kind of data. When encryption is not performed, IP packet 60 is directly transmitted to the MAC frame preparing part 22 from the IP packet preparing part 20.
[0052]Here, it describes about the case where encryption is performed. Encryption is usually performed to a 64-bit plaintext, and in not being a multiple whose data length of IP packet 60 which should be enciphered is 64 bits, the IP packet 60 whole is made into a 64-bit multiple by performing amends of data, i.e., padding of invalid data, and it considers it as IP packet 61.
[0053]IP packet 62 as which specific IP packet 61 for users was enciphered is transmitted to the MAC frame preparing part 22. In the MAC frame preparing part 22, MAC header 70 is added to IP packet 62 enciphered with the encryption machine 21.

[0054]This MAC header 70 comprises a total of 64 bits of 8 bits SSID (Server System ID), UDB(User Depend Block)1 [24 bits], and 32-bit UDB2, as shown in Fig.6. In particular, the transmission destination IP address written in the above-mentioned IP header and the same transmission destination IP address are written in UDB2 of MAC header 70.

[0055]The transmission destination IP address in the above-mentioned IP header is enciphered, in the receiving set side, if a code is not decoded, cannot know a transmission destination IP address, but if above-mentioned MAC header 70 has the same transmission destination IP address as it, At a receiving side, it can be known by reading it only in hardware whether it is a data block addressed to itself. This transmission destination IP address is directly passed to the MAC frame preparing part 22 from the IP packet preparing part 20.

[0056]To the above-mentioned UDB1, PBL (Padding_Byte_Length) of a triplet, 1 bit CP (Control_Packet) and 1-bit EN (Encrypted_or_Not), 1 bit PN (Protocol_Type Available_or_Not), 2 bits Reserve, and a 16-bit protocol number (Protocol Type) are set.

[0057]Among this, PBL is padding bite length and is the length of the invalid data covered on the occasion of encryption. This is needed in order that the user who received the enciphered IP packet may know regular data length.

[0058]CP is a bit which identifies whether the data which a user needs, or control data required for system management is contained in the IP packet. Usually, CP of MAC frame 63 which should be received when a user requests shows that not control data but data is contained.

[0059]EN is a control bit which shows whether the IP packet is enciphered with the encryption machine 21. As for a user, decoding received MAC frame 63 determines whether lends and there is by this bit information. PN is a control bit which shows whether useful information is in a Protocol Type area.

[0060]In the MAC frame preparing part 22 of Fig.3, the above control bit is added to IP packet 62. Here, the content ID showing the kind of information on an IP packet besides the above-mentioned transmission destination IP address may be set to UDB2. This content ID is mentioned later. It is the above-mentioned SSID to make it identify whether the above-mentioned transmission destination IP address was set to UDB2 or it is the above-mentioned content ID.

[0061]CRC (Cyclic Redundancy Checking, Cyclic Redundancy Check) calculated in the CRC calculation part 23 is added to MAC frame 63 generated by the MAC frame preparing part 22. Thus, by calculating CRC by the data distribution device 10 side, the data receiver 30 can inspect whether the received MAC frame is correctly transmitted from the communications satellite 18. 16-bit CRC generated in the CRC calculation part 23 is added to the last of MAC frame 63.

[0062]This MAC frame 63 is converted to the section which is transmitted to the section preparing part 24 and specified by MPEG 2. As shown in Fig.4, MAC frame 63 is added immediately after the section (Sec) header 71, and is called the private section 64.

[0063]The format of this section header 71 is shown in Fig.7 (A). The format of the section header 71 is prescribed by MPEG 2, Table (ID) It has T_{id}, section sink indicator S_{si}, private indicator P_i, reserved R_{es}, and private section length P_{sl}. Here, the data length of a MAC frame goes into private section length P_{sl}.

[0064]The private section 64 created by the section preparing part 24 is transmitted to the transport packet preparing part 25. the private section 64 transmitted in the transport packet preparing part 25 -- transport packet 65_1, 65_2, and .. it divides into 65_n.

[0065]transport packet 65_1, 65_2, and .. 65_n comprises 188 bytes, respectively. these transport packet 65_1, 65_2, and .. 4 bytes of TS header is added to 65_n.

[0066]For example, the format of the TS header 72 is shown in Fig.7 (B). The TS header 72 Sync byte S_{yb}, transport error indicator T_{ei}, Pay-load unit start indicator P_{ui}, transport priority T_p, It has above-mentioned PID and above-mentioned scramble control part (transport scramble control) T_{sc}, adaptation field control A_{fc}, and Conti ******- counter C_c.

[0067]transport packet 65_1, 65_2, and .. since it is specified with having mentioned above the size for one piece of 65_n as 188 bytes, generally it is necessary to divide the one section 64 into two or more transport packets

[0068]Since one section is not necessarily the integral multiple length of 184 bytes (number of bytes to which 4 bytes of header length were pulled from 188 bytes), usually here, the one section 64 -- two or more transport packet 65_1, 65_2, and .. when dividing into 65_n, as shown in Fig.4, the data using stuffing bytes is made up for. That is, when one section which is not 184 bytes of multiple is divided into two or more transport packets, all the bits form the stuffing region by which stuffing was carried out in the data area in which the last transport packet remained.

[0069]Each transport packet created by the transport packet preparing part 25 is supplied to the encryption machine 26. The encryption machine 26 performs encryption processing to the data part of each above-mentioned transport packet using the enciphering key for TS packets, as shown in Fig.2.

[0070]The service provider 19 gives previously the PID portion of a TS packet and the value of a scramble control part to transmit, and the decode key which decodes this TS packet to the data receiver 30. And the encryption IP packet given from contents PURABAIDA 18 is TS-packet-ized, the payload part of this TS packet is further enciphered with the encryption key corresponding to the above-mentioned decode key, an encryption TS packet is created, and it transmits on satellite connection.

[0071]Here, as mentioned above, the peculiar bit string corresponding to PID (13 bits) and the scramble control part (2 bits) of TS header which were shown in (b) of Fig.7 is used for the enciphering key for encryption. For this reason, 15-bit 4096 kinds of limitation can be performed at the maximum.

[0072]Since the addressee can be divided into the range the 32nd power of 2 as already mentioned above using the transmission destination IP address of an IP packet, if encryption of this TS packet is combined, an addressee can be further divided into that 4096 times as many range, and a warmer restricted reception system can be constituted.

[0073]Since plaintext data cannot be obtained if another code is undecipherable even if it succeeds in a tapping person decoding one of codes by performing independent encryption doubly, a restricted reception system with higher safety can be constituted.

[0074]Here, since the restricted reception system by encryption of an IP packet and the restricted reception system by encryption of a TS packet are held by another entrepreneur of the content provider 18 and the service provider 19, respectively, a restricted reception system with the independent others can be constituted. This is effective when each wants for the entrepreneur who provides a transmission line to differ from the entrepreneur who provides transmission data, and to sign a limited reception contract with a user independently. There is also no possibility that the information about an encryption key may leak among entrepreneurs.

[0075]After the data in which double encryption was given by the content provider 18 and the service provider 19 is transmitted to the data transfer part 27, it is transmitted to the data processing parts 16, such as a multiplexer. In the data processing part 16, it modulates and amplifies, after multiplexing the above-mentioned transport packet with other digitized videos and an audio signal.

[0076]The data for the broadcast specific user is received by users' receiving antenna 31, and is transmitted to a specific user's data receiver 30.

[0077]The signal received by the receiving antenna 31 is converted to the signal of IF, and is input into the data receiver 30. The block diagram of this data receiver 30 is shown in Fig.8. The flow chart of the double decoding processing performed with this data receiver 30 is shown in Fig.9.

[0078]It converts to a digital signal here, QPSK demodulation processing and error correction processing are performed, and the signal input into the front end 32 which consists of the tuner 33, A/D converter 34, the demodulator 35, and the decoder 36 is received as TS packet data enciphered like Step S1.

[0079]This enciphered TS packet is supplied to the descrambler 37. The descrambler 37 performs descrambling processing of TS packet level to the TS packet data enciphered [above-mentioned]. In this case, the descrambler 37 reads the value of a PID part and a scramble control part in the header part of the above-mentioned encryption TS packet data, It judges whether the decode key for TS packets corresponding to this value is given from the service provider 19 at Step S2, and if given, the payload part of this encryption TS packet will be decoded with this decode key at Step S3, and the decoded TS packet will be outputted. Here, if the decode key is not previously given from the service provider 19, an encryption TS packet is canceled at Step S7.

[0080]The TS packet decoded at Step S3 is supplied to the demultiplexer 38. Here, the demal plexor 38 divides the audio information and the video data which were multiplexed with the above-mentioned TS packet data by the written data processing part 16, supplies audio information to the audio decoder 39, and supplies a video data to the video decoder 40. The audio decoder 39 outputs an analog audio and the video decoder 40 outputs analog video via NTSC encoder 41. The remaining TS packet data are supplied to DEPAKETAIZA 45.

[0081]DEPAKETAIZA 45 reproduces the format of the private section 64 shown by Fig.4, calculates the value of CRC, and judges whether data was received correctly. And DEPAKETAIZA 45 IP-packet-izes the above-mentioned private section 64 by step S4, and converts it to the format data 75 as shown in Fig.10. This format data 75 is transmitted to the decoder 47 which decodes this IP packet via FIFO46.

[0082]The identifier set to UDB2 shown in the Fig.6 of the MAC header in the format data 75 in the decoder 47, Take out a transmission destination IP address here, judge whether the decode key for IP packets corresponding to this is given from contents PURABAIDA 18 at Step S5, and if given, The payload part of an IP packet is decoded using this decode key at Step S6, and the decoded IP packet is outputted. Here, if the decode key is not previously given by the content provider 18, an encryption IP packet is canceled at Step S7.

[0083]A decode key is made to correspond to the above-mentioned identifier, and is stored by the reference table 80 shown in the Fig.11 in the dual port rum (DPRAM) 48.

[0084]This reference table 80 has an identifier of the data block of a receivable kind with that identifier and a corresponding decode key. 4 bytes is used as an identifier and 8 bytes is used as a decode key.

[0085]As mentioned above as an identifier among the figure, content ID may be used, using a transmission destination IP address, and the discernment is performed by SSID in the MAC header of a receive packet. Setting out of the value of the reference table 80 is performed by CPU42 with the input of DPRAM48.

[0086]If encryption IP packet data are received in the format of the above-mentioned Fig.10 and the identifier of UDB2 in a MAC Address is taken out, the decoder 47, DPRAM48 is accessed, the identifier in the table 80 is searched at intervals of 16 bytes from a top address, and coincidence detection of the identifier in a receive packet and the identifier in a table is performed to the bit of the identifier which is "1" among the mask bits stored in 4 bytes of Ushiro of an identifier.

[0087]If the mask bit is H"ffffffff", correspondence of all the bits of the identifier in the MAC Address of the received packet and the identifier in a table will be checked, It supposes that the same identifier as the input identifier is in DPRAM48, the decode key (session key in a figure) corresponding to the identifier is taken out, and decoding processing of the IP packet after it is performed.

[0088]When the END code is stored in the last of the identifier in the reference table 80 registered previously, the identifier is searched and an END code is detected, as Step S7 showed without ejection and its receive packet receiving search there, it is discarded with this decoder 47.

[0089]As an identifier, as mentioned above, content ID (or genre ID) besides a transmission destination IP address is used. That is, content ID besides a transmission destination IP address may be set to UDB2 of MAC header 70 shown in Fig.6. When using a transmission destination IP address when "0" is set as SSID is shown, for example, "1" is set, it specifies using genre ID. It can distinguish which is used by analyzing SSID by a receiving side.
[0090]For example, individually-addressed [corresponding to a unicast address], when a transmission destination IP address is used for UDB2, and -- it becomes possible to transmit the data addressed to a group's user using a multicast address -- a receiving side -- addressing to oneself -- or it becomes possible to receive only the data addressed to a groove where he can belong and which is in real time.
[0091]In this case, DPRAM48 of the data receiver 30 should just be provided with the reference table 81 of a format as shown in Fig.12. This reference table 81 has a transmission destination IP address of the data block of a receivable kind with that transmission destination IP address and a corresponding decode key. For example, transmission destination IP address 1 for groups like the above-mentioned multicast address is set to 16 bytes to begin.
[0092]The encryption ON/OFF flag of this transmission destination IP address 1 is 0. Individually-addressed transmission destination IP address 2 like the above-mentioned unicast address is set to the following 16 bytes. An encryption ON/OFF flag is 1. The session key is set also to transmission destination IP address 2.
[0093]If the decoder 47 receives IP packet data in the format of the above-mentioned Fig.10 and inputs the transmission destination IP address in a MAC Address, Access DPRAM48 and the transmission destination IP address in the table 81 is searched at intervals of 16 bytes from a top address, Coincidence detection of the identifier in a receive packet and the identifier in a table is performed to the bit of the identifier which is "1" among the mask bits stored in 4 bytes after this IP address.
[0094]If the mask bit is H"ffffffff", correspondence of all the bits of the transmission destination IP address in the MAC Address of the received packet and the transmission destination IP address in a table will be checked, It supposes that the same IP address as the input IP address occurs in DPRAM48, the decode key corresponding to the IP address is taken out, and decoding processing of the IP packet after it is performed.
[0095]At the end of the IP address in the reference table 81 registered previously, when the END code is stored, the IP address is searched and an END code is detected, it is discarded like Step S7 with this decoder 47, without ejection and its receive packet receiving search there.
[0096]When the data of the genre previously registered on the other hand when the content ID using 32 bits was used for full as UDB2 is received, data is transmitted to PC and it becomes possible to download automatically to a hard disk.
[0097]In this case, DPRAM48 of the data receiver 30 should just be provided with the reference. table 82 of a format as shown in Fig.13. This reference table 82 has memorized the content ID 83 of the data block of a receivable kind using 32-bit full.
[0098]Such 32-bit content ID 83 is constituted by 8-bit main class D_0, classification-in 6 bits D_1, 4-bit minor class D_2, and 14-bit information ID as shown in (A) of Fig.14. Main class D_0 expresses a big category, such as computer software, a publication, and game software. Inside classification D_1 shows a middle category, such as books, a magazine, and a newspaper, if main class D_0 is a publication. Minor class D_2 shows the category showing the newspaper publishing company name of A newspaper, B newspaper, and S newspaper, if inside classification D_1 is a newspaper. And one data unit is identified by only ID in this minor class D_2. In this case, the date of issue of a newspaper serves as information ID, and it becomes content ID as shown in (B) of Fig.14 as a result.
[0099]The method of the actual information discernment at the time of using such content ID as an identifier is described below. For example, in the example of the above-mentioned Fig.14, when making a contract of A newspaper, a mask bit is made

into H"ffffc000" and this mask bit should just detect correspondence of the identifier of the receive packet of the bit position of 1, and the identifier in a table. If the mask bit is made into H"fffc0000" when it is not based on a peculiar newspaper name but receives all the newspapers, A newspaper H "02084000+ date-of-issue ID" and the B newspaper H "02088000+ date-of-issue ID" are altogether downloadable by one setting out.

[0100]If only the genre of required information is specified even if it does not specify ID of each information one by one, this will be the point that the information on the genre specified automatically is receivable, and will be a very useful method.

[0101]Since the session key to each paper cannot be set up only by setting up content ID when each information is enciphered as each paper is merely enciphered with the separate session key in this case, for example, it is an effective method when each information is not enciphered to the last.

[0102]As an identifier of the above-mentioned information, there is also a method using the MAC Address currently assigned to each product by 48 bit length.

[0103]It judges that this data block will be a data block of the kind registered previously if a transmission destination IP address and content ID can be read, and the decoder 47 extracts, and as the IP header and IP data in the format data 75 which were enciphered were mentioned above, it decodes.

[0104]The decrypted data block is transmitted to the main memory on a personal computer via FIFO49 and PCI interface 50. And processing by the software of this personal computer is made.

[0105]CPU42 controls the reading of DPRAM48 and it sets up the value of a reference table. CPU42 controls the demultiplexer 38, DPRAM48, and DPRAM52 according to the program read into RAM43 from ROM44. CPU42 may process the data read from IC card reader 53, and may generate the above-mentioned decode key. The above-mentioned request is transmitted to data supply origin with ISDN via the modem 54 and the telephone line 56.

[0106]As described above, this data receiver 30, It was set to DBU2 of a MAC frame by the data distribution device 10, and has been transmitted, Since only the data block of a transmission destination IP address and the kind which read content ID with the decoder 47 and was registered previously can be extracted, only addressing to themselves or the information to need can be extracted and decoded at high speed out of the received data which enciphered various data multiplexed.

[0107]As shown in Fig.2, it is doubly enciphered by contents propa- Ida 18 and service propa- Ida 19, and since only the data receiver 30 has two decode keys which decrypt it, the transmitted data can prevent data from being used by stealth for others.

[0108]The data transmission system used as this embodiment may be performed with composition as shows the double encryption processing by the side of the data distribution device 10 to Fig.15. That is, encryption processing of an IP packet is not made to give the content provider 18, but it is made to carry out to the service provider 19. For this reason, the content provider 18 can cut down cost.

[0109]If it constitutes so that one entrepreneur may perform both encryption processings, it will become unnecessary that is, for another entrepreneur to have the equipment for encryption processing. When two or more content providers use the transmission line which one service provider provides, for example, since each content provider does not need to have encryption disposal equipment, this is effective.

[0110]Since operation of each part is the same as operation of each part shown in Fig.2 here and the composition of the data receiver 30 is also the same, a description is omitted.

[0111]It may be made for the composition in the data receiver 30 to be shown in Fig.16. That is, it is good also as composition which provides the memory storage 58 like a hard disk driver between DEPAKETAIZA 45 and the decoder 47, and accumulates the enciphered IP packet. What is necessary is to accumulate the enciphered IP packet in the memory storage 58, and just to decode, when the above-mentioned decode key is obtained afterwards even if it has not obtained the decode key which decodes an IP packet previously if it does in this way.

[0112]That is, by saving enciphered Paquette at memory storage, even if a receiving set obtains a decode key afterwards, data can become effective. For example, by saving a lot of data previously at memory storage, obtaining a decode key in the stage which the user meant, and using data, after a user means, compared with beginning to receive data, the time for receiving a lot of data can be saved.

[0113]Here, although the case where the decode key for the receiving set 30 to decode an IP packet had not been obtained was described, even when the decode key for decoding a TS packet has not been obtained, same processing can be performed by saving the TS packet enciphered at memory storage.

[0114]Although the enciphered data can be saved, when the decoded data and a decode key add the structure which cannot be saved, it also becomes possible to prevent copying plaintext data.

[0115]Although the IP packet was considered as transmission data in each example mentioned above, even if it considers other transmission protocol packets with the same structure, the same restricted reception system is configurable. Paquette-ization of transmission data may be made or more into three-fold, and three or more restricted reception systems may be combined. For this reason, encryption processing may be performed to the file data before IP-packet-izing.

[0116]For example, the data compression method of a MAC frame is not limited to MPEG 2, but other compression methods may be used for it. Internet Protocol is not limited to TCP/IP, for example, an OSI (Open System Interconnection) system may be used for it.

[0117]

[Effect of the Invention]The information transmission equipment and the method concerning the present invention transmit this encoded data, after performing at least two-fold encryption processing including the encryption processing using the encryption key according to the identifier which shows the kind of the above-mentioned digital data to the above-mentioned digital data, Since decoding processing is performed to the above-mentioned encoded data received via the data transmission line using each decode key according to each encryption key, also when transmitting digital data using a communications satellite, the degree of leakage of information and the degree of disturbance can be made low.

[0118]The information reception equipment and the method concerning the present invention, Since only the data block of the kind which received two or more kinds of data blocks to which the identifier which shows the kind of data was added via the data transmission line, read the above-mentioned identifier, and was registered previously is extracted and decoded, A specific user can be made to receive the digital data transmitted via the data transmission line from the information distributor according to the kind of data at high speed.

[0119]Since the information storage medium concerning the present invention has memorized the encoded data in which encryption processing by the encryption key according to the identifier which shows the kind of digital data was performed at least, even if a receiving set obtains a decode key afterwards, data can be effectively used for it.

[0120]Since the information storage medium concerning the present invention memorizes two or more kinds of data blocks to which the content ID which shows the kind of data block was added, it can extract only the information to need easily.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a configuration diagram of the data transmission system used as an

embodiment of the invention.
[Drawing 2]It is a block diagram showing briefly the composition in connection with double encryption processing of a written data transmission system.
[Drawing 3]It is a block diagram showing the composition of the data creation part shown in the above-mentioned Fig.1.
[Drawing 4]It is a figure for describing the process of the data creation in the data creation part shown in the above-mentioned Fig.3.
[Drawing 5]It is a format figure showing the detailed composition of an IP header.
[Drawing 6]It is a format figure of a MAC header.
[Drawing 7]It is a format figure of a section header and TS header.
[Drawing 8]It is a block diagram of the data receiver which constitutes a written data transmission system.
[Drawing 9]It is a flow chart for describing the decoding processing performed with a written data receiving set.
[Drawing 10]It is a figure for describing transmission of the data from written data receiving set Uchi's DEPAKETAIZA to a decoder.
[Drawing 11]It is a fundamental configuration diagram of the reference table which written data receiving set Uchi's DPRAM stores.
[Drawing 12]It is a figure showing the first example of the above-mentioned reference table.
[Drawing 13]It is a figure showing the second example of the above-mentioned reference table.
[Drawing 14]It is a figure showing the example of specific constitution of content ID.
[Drawing 15]It is a block diagram showing other examples of the data distribution device in a written data transmission system.
[Drawing 16]It is a block diagram showing other examples of the data receiver in a written data transmission system.
[Drawing 17]It is a schematic structure figure showing an example of the encoded data transmission equipment which enciphers the data on a transmission line with a common key encryption system.
[Explanations of letters or numerals]
10 A data distribution device and 18 [An encryption machine, 30 data receivers, and 37 / A descrambler and 45 / DEPAKETAIZA and 47 / Decoder] A content provider and 19 A service provider and 21 An encryption machine, 25 TS-packet preparing part, and 26

CORRECTION OR AMENDMENT

[Kind of official gazette]Printing of correction by regulation of Patent Law Article 17 of 2
[Section Type] The 3rd Type of the part VII gate
[Publication date]Heisei 15(2003) June 13 (2003.6.13)

[Publication No.]JP,10-215244,A
[Date of Publication]Heisei 10(1998) August 11 (1998.8.11)
[Annual volume number] Publication of patent applications 10-2153
[Application number]Japanese Patent Application No. 9-12810
[The 7th edition of International Patent Classification]
H04L 9/14

9/36

[FI]
H04L 9/00 641

685

[Written Amendment]
[Filing date]Heisei 15(2003) February 28 (2003.2.28)
[Amendment 1]
[Document to be Amended]Description
[Item(s) to be Amended]Whole sentence
[Method of Amendment]Change
[Proposed Amendment]
[Document Name]Description
[Title of the Invention]Information transmission equipment, an information transmission method, information reception equipment, and an information receiving method
[Claim(s)]
[Claim 1]In information transmission equipment which divides digital data into a predetermined data block, and transmits this data block via a data transmission line,
A transmitting means which performs at least two-fold encryption processing, and transmits this encoded data including encryption processing using an encryption key according to an identifier which shows a kind of the above-mentioned digital data to the above-mentioned digital data,
Information transmission equipment provided with a receiving means which receives the above-mentioned encoded data transmitted via a written data transmission line from the above-mentioned transmitting means, and performs decoding processing using each decode key according to each encryption key.
[Claim 2]The information transmission equipment according to claim 1, wherein the above-mentioned predetermined data block is Paquette by Internet Protocol for transmitting and receiving digital data via a network between two or more systems.
[Claim 3]In an information transmission method which divides digital data into a predetermined data block, and transmits this data block via a data transmission line,
Encryption processing using an encryption key according to an identifier which shows a kind of the above-mentioned digital data to the above-mentioned digital data is included,
An information transmission method performing decoding processing to the above-mentioned encoded data which transmitted this encoded data after performing at least two-fold encryption processing, and was received via a written data transmission line using each decode key according to each encryption key.
[Claim 4]In information reception equipment which receives multiplexing data which consists of two or more kinds of data blocks to which an identifier which shows a kind of data was added via a data transmission line,
Information reception equipment extracting and decoding only a data block of a kind which read the above-mentioned identifier and was registered previously.
[Claim 5]The information reception equipment according to claim 4 having an identifier of a data block of a receivable kind in a reference table with the identifier and a corresponding decode key.
[Claim 6]The information reception equipment according to claim 5 characterized by performing decoding processing to this encryption data block based on a decode key according to an identifier with reference to the above-mentioned reference table when the enciphered above-mentioned data block is received.
[Claim 7]In an information receiving method which receives multiplexing data which consists of two or more kinds of data blocks to which an identifier which shows a kind of data was added via a data transmission line,
An information receiving method extracting and decoding only a data block of a kind which read the above-mentioned identifier and was registered previously.
[Claim 8]The information receiving method according to claim 7 using content ID showing a kind of information on the above-mentioned data block as the

above-mentioned identifier.
[Claim 9]The information receiving method according to claim 7 having the above-mentioned identifier in a header of media access control to which it was added by head of each data block.
[Detailed Description of the Invention]
[0001]
[Field of the Invention]The present invention relates to the information transmission equipment, the method, the information reception equipment, and the method for offering data distribution service, for example using a communications satellite.
[0002]
[Description of the Prior Art]When [which carries out data communications using a dial-up line a dedicated line, etc.] case or talking over the telephone, in order to prevent leakage of transmitted data, or in order to maintain the reliability of information to the disturbance over transmitted data, the data of the plaintext was enciphered and transmitted and the data enciphered in the reception destination is decoded.
[0003]As a typical cipher system, the common key encryption system and the public-key crypto system are known. The common key encryption system is also called the symmetrical cryptosystem, and there are an algorithm nondisclosure type and an algorithm public presentation type. DES (Date Encryption Standard) is known as a typical algorithm public presentation type thing. Since computational complexity immense in order to derive a decode key from an enciphering key is required and a decode key is not decoded substantially, a public-key crypto system is a cipher system which may exhibit an enciphering key.
It is also called an unsymmetrical key cipher system.

[0004]Fig.17 is a schematic structure figure showing an example of the encoded data transmission equipment which enciphers the data on a transmission line with a common key encryption system. This encoded data transmission equipment protects that the bugging device 93 by the side of a tapping person intercepts data from the data transmission line 94 which connects the sending set 91 by the side of a sending person, and the receiving set 92 by the side of an addressee.
[0005]Encryption processing which uses the encryption key 97 with the encryption machine 96 in the sending set 91 is performed to the data which should be transmitted. The above-mentioned encoded data which was transmitted by the data transmission line 94 and received with the receiving set 92 is decoded by the decoder 99 which used the decode key 98, and decode data is obtained.
[0006]Since it does not have the decode key 98 even if the bugging device 93 receives here the data similarly enciphered as the receiving set 92 from the data transmission line 94, it is difficult to decode. That is, in the bugging device 93, since the data which required then incomprehensible encryption processing (scramble) as it is will be treated, it can prevent leaking information to the bugging device 93 side actually. Generally in the main encryption methods of the common key encryption system in this example, an enciphering key and a decode key are identical-bits sequences.
[0007]A cipher system which was mentioned above is determined according to the classification of the circuit system to which transmission data is transmitted, the degree of secrecy (confidentiality) of transmission data, the quantity of transmission data, etc. For example, in the data communications using a dedicated line, although leakage of information and the degree of the disturbance to transmission data are low, when carrying out data communications using a dial-up line, the degree of leakage of information and the degree of disturbance become high.
[0008]
[Problem to be solved by the invention]By by the way, the thing for which transmission of the digital data using a communications satellite was attained in recent years, Although transmitted [came] using the communications satellite also about the text,

and the digital video and voice data which are used not only by analog video and voice data, such as television broadcasting and a movie, but by computer etc., Since reception with many and unspecified receiving sets is possible, the degree of leakage of information and the degree of disturbance become still higher.

[0009]That is, in the data transmission system using the above-mentioned communications satellite, since many and unspecified addressees can receive easily with a receiving set unlike 1 to 1 communication of a telephone line, a dedicated line, etc., it is easy to be intercepted. For this reason, a possibility that charged data communications will be intercepted, for example is high. Then, a data encryption is needed also a written data transmission system.

[0010]In a actual written data transmission system, encryption processing is performed about not all data, Using the information which the data which should be enciphered was enciphered according to the contents of the data which should be transmitted in a sending set, it sent out on the transmission line, and the addressee decoded all or some of enciphered data, and was acquired as a result, Or it is got to know whether the data is required for itself by the portion transmitted without being enciphered.

[0011]Here, the conventional television broadcast service using a communications satellite is a form as for which a many user uses the data which the distribution person distributed receiving it simultaneously. On the other hand, when distributing the digital data used by computer etc. via a communications satellite, the function which distributes data to the specific user of the singular number or plurality from a data distribution person is called for.

[0012]However, conventionally, in the simultaneous transmissive communication or broadcasting system from a data distribution person to many users, All Users received the always same information, use or an inspection was carried out, and since there was no identification information of a system user individual, distribution of data only to a specific user from a data distribution person was not completed.

[0013]The present invention is made in view of the above-mentioned actual condition, and also when it transmits digital data using the above-mentioned communications satellite, it aims at offer of the information transmission equipment and the method of making the degree of leakage of information, and the degree of disturbance low.

[0014]The present invention is made in view of the above-mentioned actual condition, and aims at offer of the information reception equipment and the method only a specific user enables it to receive the digital data transmitted via the data transmission line from the information distributor according to the kind of data.

[0015]

[Means for solving problem]In order that the information transmission equipment and the method concerning the present invention may solve an aforementioned problem, After performing at least two-fold encryption processing including the encryption processing using the encryption key according to the identifier which shows the kind of the above-mentioned digital data to the above-mentioned digital data, this encoded data is transmitted, Decoding processing is performed to the above-mentioned encoded data received via the data transmission line using each decode key according to each encryption key.

[0016]In order that the information storage medium concerning the present invention may solve an aforementioned problem, the encryption processing by the encryption key according to the identifier which shows the kind of digital data has memorized the encoded data given at least.

[0017]In order to solve an aforementioned problem, the information reception equipment and the method concerning the present invention receive two or more kinds of data blocks to which the identifier which shows the kind of data was added via a data transmission line, read the above-mentioned identifier, and extract and decode only the data block of the kind registered previously.

[0018]

[Mode for carrying out the invention]It describes referring to Drawings for the embodiment of the information transmission equipment concerning the present invention, a method, information reception equipment, and a method hereafter. This embodiment is a data transmission system of the Fig.1 which divides digital data into a predetermined data block, and transmits this data block via satellite connection.
[0019]This data transmission system is provided with the following.
The data distribution device 10 which performs double encryption processing and transmits this duplicate encryption data including encryption processing using an encryption key according to an identifier which shows a kind of the above-mentioned digital data to digital data.
The data receiver 30 which receives the above-mentioned duplicate encryption data transmitted via the above-mentioned satellite connection from this data distribution device 10, and performs decoding processing using each decode key according to each encryption key.
Here, the expansion slot of a personal computer is equipped with the data receiver 30, for example. The personal computer is shown in Fig.1 as the data receiver 30 as it is.
[0020]The data distribution device 10 and the data receiver 30 can communicate mutually via a terrestrial communication network like ISDN in which bidirectional communication is possible. This terrestrial communication network may be connected to the Internet which transmits and receives digital data via a network between two or more systems. The satellite connection by the communications satellite 18 has transmission capacity larger than the above-mentioned terrestrial communication network.
[0021]First, the data flow in a written data transmission system is described. Here, it is assumed that the specific user who owns the data receiver 30 with the data donor who owns the data distribution device 10 has made the contract of delivery of data previously. With the data donor here, both the entrepreneur (henceforth a content provider) who provides transmitted data, and the entrepreneur (henceforth a service provider) who provides a transmission line are included.
[0022]The user who owns the data receiver 30 sends the request of the purport that he would like to receive the predetermined service which a data donor provides to the data distribution device 10, for example via ISDN as a terrestrial communication network. The method in particular of sending this request may not be limited, but may be decided by the kind of data, or a contract state with a user, for example, mail etc. may be sufficient as it. In accordance with a contract, a data donor may provide service previously, without sending a request.
[0023]The request from a user sent to the data distribution device 10 is received by the data request reception part 11, and is sent to the data management part 12. The data management part 12 will perform the read request of data to the data accumulation part 13, if the contract information and the request of a user check that it is that meaningful and it is satisfactory. The data accumulation part 13 sends data to the data creation part 15 via the high-speed switcher 14, according to a data read demand for example.
[0024]In the data creation part 15, to the data from the data accumulation part 13, IP-packet-izing, Format conversion, such as formation of a media-access-control (Media Access Control, MAC) frame and transport-izing of MPEG(Moving Picture Experts Group Phase) 2, is performed. The data creation part 15 enciphers the above-mentioned duplex after IP-packet-izing of data, and transport-izing.
[0025]It describes below about this format conversion. As mentioned above, it becomes possible for various kinds of data like an audio, a video signal, or data to multiplex, and to be transmitted by a mass digital circuit in recent years. As the method of this multiplexing, the transport stream (Transport Stream, TS) packet which is a transmission format of MPEG 2, for example is known. In this TS packet, encryption processing has been performed to the information data part (payload part). The peculiar bit string corresponding to 13 bits packet ID (PID) of the header part of a TS packet and

a 2-bit scramble control part is used for the enciphering key for this encryption. Above-mentioned PID is used to identify information kinds, such as video of the specific channel of each TS packet, and an audio.
[0026]In transmitting data using this TS packet, data is converted to the format of the Internet Protocol (IP) packet currently widely used on the Internet, and it puts this IP packet into a TS packet further.
[0027]By the way, when various kinds of data is transmitted as an IP packet, it is used in order that above-mentioned PID may discriminate the data of an IP packet from other videos or the data of an audio, Bit length is also the number of bits insufficient for making the classification of various data which has only 13 bits and is transmitted by an IP packet identify. Then, the identifying method of kinds of data other than PID is needed.
[0028]For example, on the Internet, the transmission destination address (DestinationAddress) included in identifying whether received data are data addressed to themselves at the IP header of an IP packet is used. Even when transmitting an IP packet by a TS packet, it is possible to identify whether it is data addressed to itself using this transmission destination address (it is henceforth called a transmission destination IP address.).
[0029]However, it is dramatically difficult for a data transmission rate to serve as 30Mbps per one translator, if satellite connection is taken for an example, for example, and to analyze a transmission destination IP address by software in real time by a data receiving side. By a certain means, a means to extract only the information addressed to oneself is needed.
[0030]It is very convenient, if only the information on the genre of its interested information is specified even if it does not specify the title of specific information, and only the information on the genre is received automatically and can download.
[0031]When data is enciphered as having mentioned above in order to consider it as ability ready for receiving only at a specific member, it is necessary to decode the enciphered data in a receiving side. So, in the written data transmission system, added the identifier which shows the kind of data to the multiplexing data which consists of two or more kinds of data blocks in the data distribution device 10, and it was made to go via the communications satellite 18, and has transmitted to the data receiver 30 by the above-mentioned satellite connection. And in the data receiver 30, the above-mentioned identifier is read in hardware, and only the data of the classification registered previously which an addressee needs is extracted and decoded.
[0032]Addition of this identifier is performed by the data creation part 15 of the data distribution device 10. It is accumulated in the data accumulation part 13 in the data distribution device 10 in the state where no data which a user needs is processed. From the data management part 12, the data accumulation part 13 told that the read request of data came from the user sends the destination information of the requested data and a user to the data creation part 15 via the high-speed switcher 14 simultaneously.
[0033]Here, a user's destination information is a transmission destination IP address required for IP packet transmission. In this data transmission system, the transmission destination IP address peculiar to all the users is assigned. While the user of 1 has secured the transmission destination IP address which the user of 1 has, no users other than the user of one have.
[0034]Creation or after format conversion is carried out, the data from the data accumulation part 13 is multiplexed with other audio signals and a video signal by the data processing part 16, and is sent to the communications satellite 18 by the data creation part 15 via a wireless circuit from the transmission antenna 17 as multiplexing data.
[0035]The multiplexing data sent via the communications satellite 18 can be received by all the users who are in the situation where not only the data receiver 30 that a specific user owns but data is receivable. The data receiver 30 receives all the

multiplexing data from the communications satellite 18, and sorts out, extracts and decrypts the data according to the request which he advanced from the inside.
[0036]This data receiver 30 extracts and decodes only the data block of the kind registered previously by receiving the multiplexing data which consists of two or more kinds of data blocks to which the identifier which shows the kind of data was added via the satellite connection by the communications satellite 18, and reading the above-mentioned identifier.
[0037]Namely, the data receiver 30 receives the many data block containing the data transmitted according to the request, sorts out the data block addressed to itself, the data block which he should receive, and the data block which he can receive, and extracts it from the inside. The data receiver 30 which a user has is previously determined by the contract of a user and a data donor. Therefore, if it is usual, the characteristic data of other addressing to a user cannot be sorted out using the data receiver 30 which a user has.
[0038]However, in the written data transmission system using the communications satellite 18, since many and unspecified addressees can receive easily with a receiving set unlike 1 to 1 communication of a telephone line, a dedicated line, etc., it is easy to be intercepted. That is, a possibility that data communications will be intercepted is high. Then, a data encryption is needed also a written data transmission system.
[0039]For this reason, the data distribution device 10 is with contents propa- Ida 18 who provides information, and service propa- Ida 19 who transmits that information, and has performed double encryption processing with the encryption machine 21 and the encryption machine 26 so that it may be shown briefly [Fig.2].
[0040]Actually, this data distribution device 10 is constituted, as shown in the Fig.1 mentioned above, and each part which the content provider 18 who showed especially Fig.2, and service propa- Ida 19 have is contained in the data creation part 15 as shown in Fig.3.
[0041]The data and the IP address addressed to a specific user which have been sent from the data accumulation part 13 are sent to the transmission destination IP packet preparing part 20. In the IP packet preparing part 20, IP packet 60 shown in Fig.4 is generated using the data sent from the data accumulation part 13, and the transmission destination IP address which specifies a user at the time. The size of this IP packet 60 is prescribed by TCP/IP (Transmission Control Protocol/Internet Protocol), When the data which the user requested exceeds that size, this data is divided into two or more IP packets, and is transmitted to the following encryption machine 21.
[0042]Transmission destination IP address 74 of the user who shows Fig.5, and IP address 73 of the transmitting agency are contained in the IP header of IP packet 60 used here. Here, transmission destination IP address 74 is 32 bits.
[0043]IP packet 60 created by the IP packet preparing part 20 is transmitted to the encryption machine 21. In the encryption machine 21, the IP packet 60 whole is enciphered with the enciphering key for IP packets which an address gets to know that he is a specific user, and already gets to know mutually only at Hazama, a data donor and a specific user, at the time by 32-bit above-mentioned transmission destination IP address 74 in IP packet 60. As an encryption expression, DES (Data Encryption Standard) etc. are adopted, for example.
[0044]the limited reception by encryption of an IP packet since this encryption machine 21 performs encryption which used 32 above-mentioned bits transmission destination IP address 74 -- an addressee can be divided into the range of the 32nd power (= about 4,300 millions) individual of 2.
[0045]Here, the content provider 18 gives previously the transmission destination IP address of the IP packet to transmit, and the decode key for decoding an encryption IP packet to the data receiver 30. And the payload part of an IP packet is enciphered with the encryption key corresponding to this decode key, and it sends to the service provider 19.

[0046]However, the encryption needs to give about no data to a specific user, and encryption may not be performed depending on the kind of data. When encryption is not performed, IP packet 60 is directly transmitted to the MAC frame preparing part 22 from the IP packet preparing part 20.
[0047]Here, it describes about the case where encryption is performed. Encryption is usually performed to a 64-bit plaintext, and in not being a multiple whose data length of IP packet 60 which should be enciphered is 64 bits, the IP packet 60 whole is made into a 64-bit multiple by performing amends of data, i.e., padding of invalid data, and it considers it as IP packet 61.
[0048]IP packet 62 as which specific IP packet 61 for users was enciphered is transmitted to the MAC frame preparing part 22. In the MAC frame preparing part 22, MAC header 70 is added to IP packet 62 enciphered with the encryption machine 21.
[0049]This MAC header 70 comprises a total of 64 bits of 8 bits SSID (Server System ID), UDB(User Depend Block)1 [24 bits], and 32-bit UDB2, as shown in Fig.6. In particular, the transmission destination IP address written in the above-mentioned IP header and the same transmission destination IP address are written in UDB2 of MAC header 70.
[0050]The transmission destination IP address in the above-mentioned IP header is enciphered, in the receiving set side, if a code is not decoded, cannot know a transmission destination IP address, but if above-mentioned MAC header 70 has the same transmission destination IP address as it, At a receiving side, it can be known by reading it only in hardware whether it is a data block addressed to itself. This transmission destination IP address is directly passed to the MAC frame preparing part 22 from the IP packet preparing part 20.
[0051]To the above-mentioned UDB1, PBL (Padding_Byte_Length) of a triplet, 1 bit CP (Control_Packet) and 1-bit EN (Encrypted_or_Not), 1 bit PN (Protocol_Type Available_or_Not), 2 bits Reserve, and a 16-bit protocol number (Protocol Type) are set.
[0052]Among this, PBL is padding bite length and is the length of the invalid data covered on the occasion of encryption. This is needed in order that the user who received the enciphered IP packet may know regular data length.
[0053]CP is a bit which identifies whether the data which a user needs, or control data required for system management is contained in the IP packet. Usually, CP of MAC frame 63 which should be received when a user requests shows that not control data but data is contained.
[0054]EN is a control bit which shows whether the IP packet is enciphered with the encryption machine 21. As for a user, decoding received MAC frame 63 determines whether lends and there is by this bit information. PN is a control bit which shows whether useful information is in a Protocol Type area.
[0055]In the MAC frame preparing part 22 of Fig.3, the above control bit is added to IP packet 62. Here, the content ID showing the kind of information on an IP packet besides the above-mentioned transmission destination IP address may be set to UDB2. This content ID is mentioned later. It is the above-mentioned SSID to make it identify whether the above-mentioned transmission destination IP address was set to UDB2 or it is the above-mentioned content ID.
[0056]CRC (Cyclic Redundancy Checking, Cyclic Redundancy Check) calculated in the CRC calculation part 23 is added to MAC frame 63 generated by the MAC frame preparing part 22. Thus, by calculating CRC by the data distribution device 10 side, the data receiver 30 can inspect whether the received MAC frame is correctly transmitted from the communications satellite 18. 16-bit CRC generated in the CRC calculation part 23 is added to the last of MAC frame 63.
[0057]This MAC frame 63 is converted to the section which is transmitted to the section preparing part 24 and specified by MPEG 2. As shown in Fig.4, MAC frame 63 is added immediately after the section (Sec) header 71, and is called the private section 64.

[0058]The format of this section header 71 is shown in Fig.7 (A). The format of the section header 71 is prescribed by MPEG 2, It has table (ID) T_{id}, section sink indicator S_{si}, private indicator P_i, reserved R_{es}, and private section length P_{sl}. Here, the data length of a MAC frame goes into private section length P_{sl}.
[0059]The private section 64 created by the section preparing part 24 is transmitted to the transport packet preparing part 25. the private section 64 transmitted in the transport packet preparing part 25 -- transport packet 65_1, 65_2, and .. it divides into 65_n.
[0060]transport packet 65_1, 65_2, and .. 65_n comprises 188 bytes, respectively. These transport packet 65_1, 65_2, -- 4 bytes of TS header is added to 65_n.
[0061]For example, the format of the TS header 72 is shown in Fig.7 (B). The TS header 72 Sync byte S_{yb}, transport error indicator T_{ei}, Pay-load unit start indicator P_{ui}, It has transport priority T_p, above-mentioned PID, the above-mentioned scramble control part (transport scramble control) T_{sc}, adaptation field control A_{fc}, and Conti ******-counter C_c.
[0062]transport packet 65_1, 65_2, and .. since it is specified with having mentioned above the size for one piece of 65_n as 188 bytes, generally it is necessary to divide the one section 64 into two or more transport packets
[0063]Since one section is not necessarily the integral multiple length of 184 bytes (number of bytes to which 4 bytes of header length were pulled from 188 bytes), usually here, the one section 64 -- two or more transport packet 65_1, 65_2, and .. when dividing into 65_n, as shown in Fig.4, the data using stuffing bytes is made up for. That is, when one section which is not 184 bytes of multiple is divided into two or more transport packets, all the bits form the stuffing region by which stuffing was carried out in the data area in which the last transport packet remained.
[0064]Each transport packet created by the transport packet preparing part 25 is supplied to the encryption machine 26. The encryption machine 26 performs encryption processing to the data part of each above-mentioned transport packet using the enciphering key for TS packets, as shown in Fig.2.
[0065]The service provider 19 gives previously the PID portion of a TS packet and the value of a scramble control part to transmit, and the decode key which decodes this TS packet to the data receiver 30. And the encryption IP packet given from contents PURABAIDA 18 is TS-packet-ized, the payload part of this TS packet is further enciphered with the encryption key corresponding to the above-mentioned decode key, an encryption TS packet is created, and it transmits on satellite connection.
[0066]Here, as mentioned above, the peculiar bit string corresponding to PID (13 bits) and the scramble control part (2 bits) of TS header which were shown in (b) of Fig.7 is used for the enciphering key for encryption. For this reason, 15-bit 4096 kinds of limitation can be performed at the maximum.
[0067]Since the addressee can be divided into the range the 32nd power of 2 as already mentioned above using the transmission destination IP address of an IP packet, if encryption of this TS packet is combined, an addressee can be further divided into that 4096 times as many range, and a warmer restricted reception system can be constituted.
[0068]Since plaintext data cannot be obtained if another code is undecipherable even if it succeeds in a tapping person decoding one of codes by performing independent encryption doubly, a restricted reception system with higher safety can be constituted.
[0069]Here, since the restricted reception system by encryption of an IP packet and the restricted reception system by encryption of a TS packet are held by another entrepreneur of the content provider 18 and the service provider 19, respectively, a restricted reception system with the independent others can be constituted. This is effective when each wants for the entrepreneur who provides a transmission line to differ from the entrepreneur who provides transmission data, and to sign a limited reception contract with a user independently. There is also no possibility that the information about an encryption key may leak among entrepreneurs.
[0070]After the data in which double encryption was given by the content provider 18

and the service provider 19 is transmitted to the data transfer part 27, it is transmitted to the data processing parts 16, such as a multiplexer. In the data processing part 16, it modulates and amplifies, after multiplexing the above-mentioned transport packet with other digitized videos and an audio signal.

[0071]The data for the broadcast specific user is received by users' receiving antenna 31, and is transmitted to a specific user's data receiver 30.

[0072]The signal received by the receiving antenna 31 is converted to the signal of IF, and is input into the data receiver 30. The block diagram of this data receiver 30 is shown in Fig.8. The flow chart of the double decoding processing performed with this data receiver 30 is shown in Fig.9.

[0073]It converts to a digital signal here, QPSK demodulation processing and error correction processing are performed, and the signal input into the front end 32 which consists of the tuner 33, A/D converter 34, the demodulator 35, and the decoder 36 is received as TS packet data enciphered like Step S1.

[0074]This enciphered TS packet is supplied to the descrambler 37. The descrambler 37 performs descrambling processing of TS packet level to the TS packet data enciphered [above-mentioned]. In this case, the descrambler 37 reads the value of a PID part and a scramble control part in the header part of the above-mentioned encryption TS packet data, It judges whether the decode key for TS packets corresponding to this value is given from the service provider 19 at Step S2, and if given, the payload part of this encryption TS packet will be decoded with this decode key at Step S3, and the decoded TS packet will be outputted. Here, if the decode key is not previously given from the service provider 19, an encryption TS packet is canceled at Step S7.

[0075]The TS packet decoded at Step S3 is supplied to the demultiplexer 38. Here, the demal plexor 38 divides the audio information and the video data which were multiplexed with the above-mentioned TS packet data by the written data processing part 16, supplies audio information to the audio decoder 39, and supplies a video data to the video decoder 40. The audio decoder 39 outputs an analog audio and the video decoder 40 outputs analog video via NTSC encoder 41. The remaining TS packet data are supplied to DEPAKETAIZA 45.

[0076]DEPAKETAIZA 45 reproduces the format of the private section 64 shown by Fig.4, calculates the value of CRC, and judges whether data was received correctly. And DEPAKETAIZA 45 IP-packet-izes the above-mentioned private section 64 by step S4, and converts it to the format data 75 as shown in Fig.10. This format data 75 is transmitted to the decoder 47 which decodes this IP packet via FIFO46.

[0077]The identifier set to UDB2 shown in the Fig.6 of the MAC header in the format data 75 in the decoder 47, Take out a transmission destination IP address here, judge whether the decode key for IP packets corresponding to this is given from contents PURABAIDA 18 at Step S5, and if given, The payload part of an IP packet is decoded using this decode key at Step S6, and the decoded IP packet is outputted. Here, if the decode key is not previously given by the content provider 18, an encryption IP packet is canceled at Step S7.

[0078]A decode key is made to correspond to the above-mentioned identifier, and is stored by the reference table 80 shown in the Fig.11 in the dual port rum (DPRAM) 48.

[0079]This reference table 80 has an identifier of the data block of a receivable kind with that identifier and a corresponding decode key. 4 bytes is used as an identifier and 8 bytes is used as a decode key.

[0080]As mentioned above as an identifier among the figure, content ID may be used, using a transmission destination IP address, and the discernment is performed by SSID in the MAC header of a receive packet. Setting out of the value of the reference table 80 is performed by CPU42 with the input of DPRAM48.

[0081]If encryption IP packet data are received in the format of the above-mentioned Fig.10 and the identifier of UDB2 in a MAC Address is taken out, the decoder 47, DPRAM48 is accessed, the identifier in the table 80 is searched at intervals of 16 bytes

from a top address, and coincidence detection of the identifier in a receive packet and the identifier in a table is performed to the bit of the identifier which is "1" among the mask bits stored in 4 bytes after an identifier.
[0082]If the mask bit is H"ffffffff", correspondence of all the bits of the identifier in the MAC Address of Paquette who received, and the identifier in a table will be checked, It supposes that the same identifier as the input identifier is in DPRAM48, the decode key (session key in a figure) corresponding to the identifier is taken out, and decoding processing of the IP packet after it is performed.
[0083]When the END code is stored in the last of the identifier in the reference table 80 registered previously, the identifier is searched and an END code is detected, as Step S7 showed without ejection and its receive packet receiving search there, it is discarded with this decoder 47.
[0084]As an identifier, as mentioned above, content ID (or genre ID) besides a transmission destination IP address is used. That is, content ID besides a transmission destination IP address may be set to UDB2 of MAC header 70 shown in Fig.6. When using a transmission destination IP address when "0" is set as SSID is shown, for example, "1" is set, it specifies using genre ID. It can distinguish which is used by analyzing SSID by a receiving side.
[0085]For example, individually-addressed [corresponding to a unicast address], when a transmission destination IP address is used for UDB2, and -- it becomes possible to transmit the data addressed to a group's user using a multicast address -- a receiving side -- addressing to oneself -- or it becomes possible to receive only the data addressed to a groove where he can belong and which is in real time.
[0086]In this case, DPRAM48 of the data receiver 30 should just be provided with the reference table 81 of a format as shown in Fig.12. This reference table 81 has a transmission destination IP address of the data block of a receivable kind with that transmission destination IP address and a corresponding decode key. For example, transmission destination IP address 1 for groups like the above-mentioned multicast address is set to 16 bytes to begin.
[0087]Encryption ON/OFF Flagg of this transmission destination IP address 1 is 0. Individually-addressed transmission destination IP address 2 like the above-mentioned unicast address is set to the following 16 bytes. Encryption ON/OFF Flagg is 1. The session key is set also to transmission destination IP address 2.
[0088]If the decoder 47 receives IP packet data in the format of the above-mentioned Fig.10 and inputs the transmission destination IP address in a MAC Address, Access DPRAM48 and the transmission destination IP address in the table 81 is searched at intervals of 16 bytes from a top address, Coincidence detection of the identifier in a receive packet and the identifier in a table is performed to the bit of the identifier which is "1" among the mask bits stored in 4 bytes after this IP address.
[0089]If the mask bit is H"ffffffff", correspondence of all the bits of the transmission destination IP address in the MAC Address of the received packet and the transmission destination IP address in a table will be checked, It supposes that the same IP address as the input IP address occurs in DPRAM48, the decode key corresponding to the IP address is taken out, and decoding processing of the IP packet after it is performed.
[0090]At the end of the IP address in the reference table 81 registered previously, when the END code is stored, the IP address is searched and an END code is detected, it is discarded like Step S7 with this decoder 47, without ejection and its receive packet receiving search there.
[0091]When the data of the genre previously registered on the other hand when the content ID using 32 bits was used for full as UDB2 is received, data is transmitted to PC and it becomes possible to download automatically to a hard disk.
[0092]In this case, DPRAM48 of the data receiver 30 should just be provided with the reference table 82 of a format as shown in Fig.13. This reference table 82 has memorized the content ID 83 of the data block of a receivable kind using 32-bit full.

[0093]Such 32-bit content ID 83 is constituted by 8-bit main class D_0, classification-in 6 bits D_1, 4 bits minor class D_2, and 14-bit information ID as shown in (A) of Fig.14. Main class D_0 expresses a big category, such as computer software, a publication, and game software. Inside classification D_1 shows a middle category, such as books, a magazine, and a newspaper, if main class D_0 is a publication. Minor class D_2 shows the category showing the newspaper publishing company name of A newspaper, B newspaper, and S newspaper, if inside classification D_1 is a newspaper. And one data unit is identified by only ID in this minor class D_2. In this case, the date of issue of a newspaper serves as information ID, and it becomes content ID as shown in (B) of Fig.14 as a result.
[0094]The method of the actual information discernment at the time of using such content ID as an identifier is described below. For example, in the example of the above-mentioned Fig.14, when making a contract of A newspaper, a mask bit is made into H"ffffc000" and this mask bit should just detect correspondence of the identifier of the receive packet of the bit position of 1, and the identifier in a table. If the mask bit is made into H"fffc0000" when it is not based on a peculiar newspaper name but receives all the newspapers, A newspaper H "02084000+ date-of-issue ID" and the B newspaper H "02088000+ date-of-issue ID" are altogether downloadable by one setting out.
[0095]If only the genre of required information is specified even if it does not specify ID of each information one by one, this will be the point that the information on the genre specified automatically is receivable, and will be a very useful method.
[0096]Since the session key to each paper cannot be set up only by setting up content ID when each information is enciphered as each paper is merely enciphered with the separate session key in this case, for example, it is an effective method when each information is not enciphered to the last.
[0097]As an identifier of the above-mentioned information, there is also a method using the MAC Address currently assigned to each product by 48 bit length.
[0098]It judges that this data block will be a data block of the kind registered previously if a transmission destination IP address and content ID can be read, and the decoder 47 extracts, and as the IP header and IP data in the format data 75 which were enciphered were mentioned above, it decodes.
[0099]The decrypted data block is transmitted to the main memory on a personal computer via FIFO49 and PCI interface 50. And processing by the software of this personal computer is made.
[0100]CPU42 controls the reading of DPRAM48 and it sets up the value of a reference table. CPU42 controls the demultiplexer 38, DPRAM48, and DPRAM52 according to the program read into RAM43 from ROM44. CPU42 may process the data read from IC card reader 53, and may generate the above-mentioned decode key. The above-mentioned request is transmitted to data supply origin with ISDN via the modem 54 and the telephone line 56.
[0101]As described above, this data receiver 30, It was set to DBU2 of a MAC frame by the data distribution device 10, and has been transmitted, Since only the data block of a transmission destination IP address and the kind which read content ID with the decoder 47 and was registered previously can be extracted, only addressing to themselves or the information to need can be extracted and decoded at high speed out of the received data which enciphered various data multiplexed.
[0102]As shown in Fig.2, it is doubly enciphered by contents propa- Ida 18 and service propa- Ida 19, and since only the data receiver 30 has two decode keys which decrypt it, the transmitted data can prevent data from being used by stealth for others.
[0103]The data transmission system used as this embodiment may be performed with composition as shows the double encryption processing by the side of the data distribution device 10 to Fig.15. That is, encryption processing of an IP packet is not made to give the content provider 18, but it is made to carry out to the service provider 19. For this reason, the content provider 18 can cut down cost.

[0104]If it constitutes so that one entrepreneur may perform both encryption processings, it will become unnecessary that is, for another entrepreneur to have the equipment for encryption processing. When two or more content providers use the transmission line which one service provider provides, for example, since each content provider does not need to have encryption disposal equipment, this is effective.
[0105]Since operation of each part is the same as operation of each part shown in Fig.2 here and the composition of the data receiver 30 is also the same, a description is omitted. It may be made for the composition in the data receiver 30 to be shown in Fig.16. That is, it is good also as composition which provides the memory storage 58 like a hard disk driver between DEPAKETAIZA 45 and the decoder 47, and accumulates the enciphered IP packet. What is necessary is to accumulate the enciphered IP packet in the memory storage 58, and just to decode, when the above-mentioned decode key is obtained afterwards even if it has not obtained the decode key which decodes an IP packet previously if it does in this way.
[0106]That is, by saving the enciphered packet at memory storage, even if a receiving set obtains a decode key afterwards, data can become effective. For example, by saving a lot of data previously at memory storage, obtaining a decode key in the stage which the user meant, and using data, after a user means, compared with beginning to receive data, the time for receiving a lot of data can be saved.
[0107]Here, although the case where the decode key for the receiving set 30 to decode an IP packet had not been obtained was described, even when the decode key for decoding a TS packet has not been obtained, same processing can be performed by saving the TS packet enciphered at memory storage.
[0108]Although the enciphered data can be saved, when the decoded data and a decode key add the structure which cannot be saved, it also becomes possible to prevent copying plaintext data.
[0109]Although the IP packet was considered as transmission data in each example mentioned above, even if it considers other transmission protocol packets with the same structure, the same restricted reception system is configurable. Packet-ization of transmission data may be made or more into three-fold, and three or more restricted reception systems may be combined. For this reason, encryption processing may be performed to the file data before IP-packet-izing.
[0110]For example, the data compression method of a MAC frame is not limited to MPEG 2, but other compression methods may be used for it. Internet Protocol is not limited to TCP/IP, for example, an OSI (Open System Interconnection) system may be used for it.
[0111]
[Effect of the Invention]The information transmission equipment and the method concerning the present invention transmit this encoded data, after performing at least two-fold encryption processing including the encryption processing using the encryption key according to the identifier which shows the kind of the above-mentioned digital data to the above-mentioned digital data, Since decoding processing is performed to the above-mentioned encoded data received via the data transmission line using each decode key according to each encryption key, also when transmitting digital data using a communications satellite, the degree of leakage of information and the degree of disturbance can be made low.
[0112]The information reception equipment and the method concerning the present invention, Since only the data block of the kind which received two or more kinds of data blocks to which the identifier which shows the kind of data was added via the data transmission line, read the above-mentioned identifier, and was registered previously is extracted and decoded, A specific user can be made to receive the digital data transmitted via the data transmission line from the information distributor according to the kind of data at high speed.
[Brief Description of the Drawings]

[Drawing 1]It is a configuration diagram of the data transmission system used as an embodiment of the invention.
[Drawing 2]It is a block diagram showing briefly the composition in connection with double encryption processing of a written data transmission system.
[Drawing 3]It is a block diagram showing the composition of the data creation part shown in the above-mentioned Fig.1.
[Drawing 4]It is a figure for describing the process of the data creation in the data creation part shown in the above-mentioned Fig.3.
[Drawing 5]It is a format figure showing the detailed composition of an IP header.
[Drawing 6]It is a format figure of a MAC header.
[Drawing 7]It is a format figure of a section header and TS header.
[Drawing 8]It is a block diagram of the data receiver which constitutes a written data transmission system.
[Drawing 9]It is a flow chart for describing the decoding processing performed with a written data receiving set.
[Drawing 10]It is a figure for describing transmission of the data from DEPAKETAIZA in a written data receiving set to a decoder.
[Drawing 11]It is a fundamental configuration diagram of the reference table which DPRAM in a written data receiving set stores.
[Drawing 12]It is a figure showing the first example of the above-mentioned reference table.
[Drawing 13]It is a figure showing the second example of the above-mentioned reference table.
[Drawing 14]It is a figure showing the example of specific constitution of content ID.
[Drawing 15]It is a block diagram showing other examples of the data distribution device in a written data transmission system.
[Drawing 16]It is a block diagram showing other examples of the data receiver in a written data transmission system.
[Drawing 17]It is a schematic structure figure showing an example of the encoded data transmission equipment which enciphers the data on a transmission line with a common key encryption system.
[Explanations of letters or numerals]
10 A data distribution device and 18 [An encryption machine, 30 data receivers, and 37 / A descrambler and 45 / DEPAKETAIZA and 47 / Decoder] A content provider and 19 A service provider and 21 An encryption machine, 25 TS-packet preparing part, and 26

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－215244

(43)公開日　平成10年(1998) 8月11日

(51)Int.Cl.6		識別記号	FI		
H04L	9/14		H04L	9/00	641
	9/36				685

審査請求　未請求　請求項の数33　ＯＬ　（全 18 頁）

(21)出願番号　特願平9－12810

(22)出願日　平成９年(1997) 1月27日

(31)優先権主張番号　特願平8－316726

(32)優先日　平８(1996)11月27日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　窪田　一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

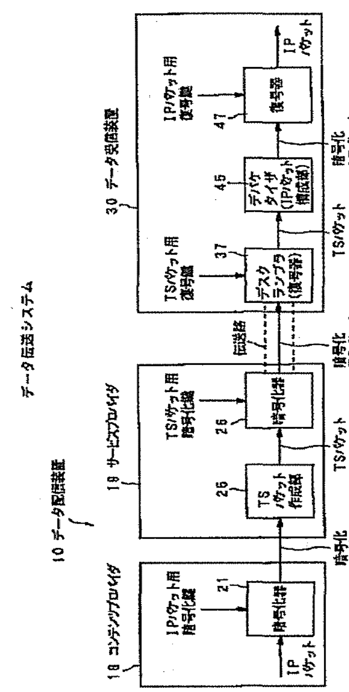
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　情報伝送装置及び方法並びに情報受信装置及び方法並びに情報記憶媒体

(57)【要約】

【課題】　通信衛星を用いるデータ伝送システムでは、不特定多数の受信装置での受信が可能であるので盗聴、妨害されやすい。

【解決手段】　データ配信装置１０は、ディジタルデータに該ディジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含め、２重の暗号化処理を施し、この２重暗号化データを送信する。データ受信装置３０は、データ配信装置１０から衛星回線を介して送信された上記２重暗号化データを受信し、それぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施す。



【特許請求の範囲】

【請求項１】　ディジタルデータを所定のデータブロックに分割し、該データブロックをデータ伝送路を介して伝送する情報伝送装置において、
上記ディジタルデータに上記ディジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含め、少なくとも２重の暗号化処理を施し、この暗号化データを送信する送信手段と、
上記送信手段から上記データ伝送路を介して送信された上記暗号化データを受信し、それぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号化処理を施す受信手段とを備えることを特徴とする情報伝送装置。

【請求項２】　上記所定のデータブロックは、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルによるパケットであることを特徴とする請求項１記載の情報伝送装置。

【請求項３】　上記受信手段は、受信した上記暗号化データを全て復号化する前に、上記データを一時的に記憶手段に保存することを特徴とする請求項１記載の情報伝送装置。

【請求項４】　上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備えることを特徴とする請求項１記載の情報伝送装置。

【請求項５】　上記データ伝送路として上記双方向データ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項４記載の情報伝送装置。

【請求項６】　ディジタルデータを所定のデータブロックに分割し、該データブロックをデータ伝送路を介して伝送する情報伝送方法において、
上記ディジタルデータに上記ディジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含め、少なくとも２重の暗号化処理を施してからこの暗号化データを送信し、上記データ伝送路を介して受信した上記暗号化データにそれぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号化処理を施すことを特徴とする情報伝送方法。

【請求項７】　上記所定のデータブロックは、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルによるパケットであることを特徴とする請求項６記載の情報伝送方法。

【請求項８】　受信した上記暗号化データを全て復号化する前に、上記データを一時的に記憶媒体に保存することを特徴とする請求項６記載の情報伝送方法。

【請求項９】　上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備えることを特徴とする請求項６記載の情報伝送方法。

【請求項１０】　上記データ伝送路として上記双方向データ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項９記載の情報伝送方法。

【請求項１１】　ディジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理が少なくとも施された暗号化データを記憶していることを特徴とする情報記憶媒体。

【請求項１２】　データの種類を示す識別子が付加された複数種類のデータブロックよりなる多重化データをデータ伝送路を介して受信する情報受信装置において、
上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号することを特徴とする情報受信装置。

【請求項１３】　受信可能な種類のデータブロックの識別子をその識別子と対応する復号鍵と共に参照テーブルに持つことを特徴とする請求項１２記載の情報受信装置。

【請求項１４】　暗号化された上記データブロックを受信したときには、上記参照テーブルを参照し、識別子に応じた復号鍵に基づいて復号処理を該暗号化データブロックに対して施すことを特徴とする請求項１３記載の情報受信装置。

【請求項１５】　上記データブロックとして、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルによるパケットを用いることを特徴とする請求項１２記載の情報受信装置。

【請求項１６】　上記識別子として、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルパケットのヘッダに含まれる送信先アドレスを用いることを特徴とする請求項１２記載の情報受信装置。

【請求項１７】　上記識別子として、上記データブロックの情報の種類を表すコンテンツＩＤを用いることを特徴とする請求項１２記載の情報受信装置。

【請求項１８】　上記識別子を各データブロックの先頭に付加されたメディアアクセス制御ヘッダの中に持つことを特徴とする請求項１２記載の情報受信装置。

【請求項１９】　上記各データブロックの先頭に付加された上記メディアアクセス制御ヘッダの中に上記識別子の種別を表すためのフラグを持つことを特徴とする請求項１８記載の情報受信装置。

【請求項２０】　上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備えることを特徴とする請求項１２記載の情報受信装置。

【請求項２１】　上記データ伝送路として上記双方向データ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項１２記載の情報受信装置。

【請求項２２】　データの種類を示す識別子が付加され

た複数種類のデータブロックよりなる多重化データをデータ伝送路を介して受信する情報受信方法において、
上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号することを特徴とする情報受信方法。
【請求項２３】　受信可能な種類のデータブロックの識別子をその識別子と対応する復号鍵と共に参照テーブルに持つことを特徴とする請求項２２記載の情報受信方法。
【請求項２４】　暗号化された上記データブロックを受信したときには、上記参照テーブルを参照し、識別子に応じた復号鍵に基づいて復号処理を該暗号化データブロックに対して施すことを特徴とする請求項２３記載の情報受信方法。
【請求項２５】　上記データブロックとして、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルによるパケットを用いることを特徴とする請求項２２記載の情報受信方法。
【請求項２６】　上記識別子として、上記インターネットプロトコルパケットのヘッダに含まれる送信先アドレスを用いることを特徴とする請求項２２記載の情報受信方法。
【請求項２７】　上記識別子として、上記データブロックの情報の種類を表すコンテンツＩＤを用いることを特徴とする請求項２２記載の情報受信方法。
【請求項２８】　上記識別子を各データブロックの先頭に付加されたメディアアクセス制御のヘッダの中に持つことを特徴とする請求項２２記載の情報受信方法。
【請求項２９】　上記各データブロックの先頭に付加された上記メディアアクセス制御ヘッダの中に上記識別子の種別を表すためのフラグを持つことを特徴とする請求項２８記載の情報受信方法。
【請求項３０】　上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を用いることを特徴とする請求項２２記載の情報受信方法。
【請求項３１】　上記データ伝送路として上記双方向データ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項３０記載の情報受信方法。
【請求項３２】　データブロックの情報の種類を示すコンテンツＩＤが付加された複数種類のデータブロックを記憶することを特徴とする情報記憶媒体。
【請求項３３】　上記コンテンツＩＤは、各データブロックの先頭に付加されたメディアアクセス制御ヘッダの中のフラグにより判別されることを特徴とする請求項３２記載の情報記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば、通信衛星を用いて、データ配信サービスを行うための情報伝送装置及び方法並びに情報受信装置及び方法並びに情報記憶媒体に関する。
【０００２】
【従来の技術】公衆電話回線、専用回線などを用いてデータ伝送する場合又は通話する場合、伝送情報の漏洩を防止するため又は伝送情報に対する妨害に対して情報の信頼性を維持するため、平文のデータを暗号化して伝送し、受信先で暗号化されたデータを復号している。
【０００３】代表的な暗号方式としては、共通鍵暗号方式と公開鍵暗号方式とが知られている。共通鍵暗号方式は対称暗号系とも呼ばれており、アルゴリズム非公開型とアルゴリズム公開型がある。アルゴリズム公開型の代表的なものとして、ＤＥＳ（Date Encryption Standard）が知られている。公開鍵暗号方式は、暗号化鍵から復号鍵を導出するために莫大な計算量が必要なため実質的に復号鍵が解読されないので、暗号化鍵を公開してもよい暗号方式であり、非対称鍵暗号方式ともよばれている。
【０００４】図１７は、伝送路上のデータを共通鍵暗号方式で暗号化する暗号化データ伝送装置の一例を示す概略構成図である。この暗号化データ伝送装置は、送信者側の送信装置９１と、受信者側の受信装置９２とをつなぐデータ伝送路９４から盗聴者側の盗聴装置９３がデータを盗聴するのを防ぐ。
【０００５】伝送すべきデータには、送信装置９１内の暗号化器９６により暗号鍵９７を用いての暗号化処理が施される。データ伝送路９４により伝送されて受信装置９２で受信された上記暗号化データは、復号鍵９８を用いた復号器９９により復号されて、復号データが得られる。
【０００６】ここで、盗聴装置９３がデータ伝送路９４から受信装置９２と同様に暗号化されたデータを受信しても、復号鍵９８を持たないので、復号することが困難である。すなわち、盗聴装置９３では、そのままでは意味不明の暗号化処理（スクランブル）のかかったデータを扱うことになるから、現実的に盗聴装置９３側に情報が漏洩することを防ぐことができる。この例における共通鍵暗号方式の主要な暗号化方法では、一般に暗号化鍵と復号鍵は同一ビット列である。
【０００７】なお、上述したような、暗号化方式は、伝送データが伝送される回線系統の種別、伝送データの機密度（機密性）、伝送データの量などに応じて決定される。例えば、専用回線を用いたデータ伝送においては、情報の漏洩、伝送データへの妨害の度合いは低いが、公衆電話回線を用いてデータ伝送する場合は情報の漏洩の度合い、妨害の度合いは高くなる。
【０００８】
【発明が解決しようとする課題】ところで、近年、通信衛星を用いたディジタルデータの伝送が可能になったこ

とで、テレビジョン放送や映画などのアナログ映像・音声データのみならず、コンピュータなどで利用されるテキストやディジタル映像・音声データについても、通信衛星を用いて伝送されるようになったが、不特定多数の受信装置での受信が可能であることから情報の漏洩の度合い、妨害の度合いは一層高くなる。

【０００９】すなわち、上記通信衛星を用いるデータ伝送システムでは、電話回線、専用回線などの１対１通信と異なり、不特定多数の受信者が受信装置で容易に受信できるので、盗聴されやすい。このため、例えば有料のデータ伝送が盗聴される可能性が高い。そこで、上記データ伝送システムでも、データの暗号化が必要とされる。

【００１０】実際の上記データ伝送システムにおいては、全てのデータについて暗号化処理を施すのではなく、送信装置において伝送すべきデータの内容に応じて、暗号化すべきデータを暗号化して伝送路上に送出し、受信者は暗号化されたデータの全部又は一部を復号して、その結果得られた情報により、或いは、暗号化されずに伝送された部分により、そのデータが自分にとって必要なものであるか否かを知る。

【００１１】ここで、通信衛星を使った従来のテレビジョン放送サービスは、配信者が配信したデータを同時に多数のユーザが受信して使用する形態である。これに対して、コンピュータなどで使用されるディジタルデータを、通信衛星を介して配信する場合には、データ配信者から単数または複数の特定のユーザにデータを配信する機能が求められる。

【００１２】しかし、従来、データ配信者から多ユーザへの同時通信又は放送システムでは、全ユーザは常に同じ情報を受信して使用又は閲覧をしており、システムユーザ個人の識別情報がないため、データ配信者から特定ユーザのみへのデータの配信ができなかった。

【００１３】本発明は、上記実情に鑑みてなされたものであり、上記通信衛星を用いてディジタルデータを伝送する際にも、情報の漏洩の度合い、妨害の度合いを低くできる情報伝送装置及び方法の提供を目的とする。

【００１４】また、本発明は、上記実情に鑑みてなされたものであり、情報配信者からデータ伝送路を介して伝送されたディジタルデータを、データの種類に応じて特定のユーザのみが受信できるようにする情報受信装置及び方法の提供を目的とする。

【００１５】また、本発明は、上記実情に鑑みてなされたものであり、少なくとも情報送信者側でディジタルデータの識別子に応じた暗号鍵により、暗号化された暗号化データを記憶している情報記憶媒体の提供を目的とする。

【００１６】また、本発明は、上記実情に鑑みてなされたものであり、情報配信者からデータ伝送路を介して伝送されたディジタルデータを、データの種類に応じたコンテンツＩＤと共に、記憶している情報記憶媒体の提供を目的とする。

【００１７】

【課題を解決するための手段】本発明に係る情報伝送装置及び方法は、上記課題を解決するために、上記ディジタルデータに上記ディジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含めた少なくとも２重の暗号化処理を施してからこの暗号化データを送信し、データ伝送路を介して受信した上記暗号化データにそれぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施す。

【００１８】また、本発明に係る情報記憶媒体は、上記課題を解決するために、ディジタルデータの種類を示す識別子に応じた暗号鍵による暗号化処理が少なくとも施された暗号化データを記憶している。

【００１９】また、本発明に係る情報受信装置及び方法は、上記課題を解決するために、データの種類を示す識別子が付加された複数種類のデータブロックをデータ伝送路を介して受信し、上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号する。

【００２０】また、本発明に係る情報記憶媒体は、上記課題を解決するために、データブロックの情報の種類を示すコンテンツＩＤが付加された複数種類のデータブロックを記憶する。

【００２１】

【発明の実施の形態】以下、本発明に係る情報伝送装置及び方法並びに情報受信装置及び方法並びに情報記憶媒体の実施の形態について図面を参照しながら説明する。この実施の形態は、ディジタルデータを所定のデータブロックに分割し、該データブロックを衛星回線を介して伝送する図１のデータ伝送システムである。

【００２２】このデータ伝送システムは、ディジタルデータに上記ディジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含め、２重の暗号化処理を施し、この２重暗号化データを送信するデータ配信装置１０と、このデータ配信装置１０から上記衛星回線を介して送信された上記２重暗号化データを受信し、それぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施すデータ受信装置３０とを備えてなる。ここで、データ受信装置３０は、例えばパーソナルコンピュータの拡張スロットに装着される。なお、図１には、パーソナルコンピュータをそのままデータ受信装置３０として示している。

【００２３】データ配信装置１０及びデータ受信装置３０は、双方向の通信が可能な例えばＩＳＤＮのような地上通信網を介して相互に通信が可能である。この地上通信網は、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うインターネットに接続されていてもよい。また、通信衛星１８による衛星回線は、上記地上通信網よりも伝送容量が大きい。

【００２４】先ず、上記データ伝送システムにおけるデータの流れを説明する。ここでは、データ配信装置１０を所有するデータ提供者とデータ受信装置３０を所有する特定のユーザが、データの配送の契約を予め結んでいるものとする。なお、ここでいうデータ提供者とは、伝送情報を提供する事業者（以下、コンテンツプロバイダという）と、伝送路を提供する事業者（以下、サービスプロバイダという）の両方を含めている。

【００２５】データ受信装置３０を所有するユーザは、例えば、地上通信網としてのＩＳＤＮを介して、データ提供者が提供する所定のサービスを受けたい旨のリクエストをデータ配信装置１０に送る。このリクエストを送る方法は、特に、限定されず、データの種類やユーザとの契約状況によって決められ、例えば郵便などでもよい。また、リクエストを送らずに、予め契約に従って、データ提供者がサービスを提供してもよい。

【００２６】データ配信装置１０に送られたユーザからのリクエストは、データリクエスト受付部１１で受け取られ、データ管理部１２に送られる。データ管理部１２は、ユーザの契約情報やリクエストが意味のあるものか否かのチェックを行い、問題が無ければ、データ蓄積部１３にデータの読み出し要求を行う。データ蓄積部１３は、データ読み出し要求に応じた、例えばデータを高速スイッチャ１４を介してデータ作成部１５に送る。

【００２７】データ作成部１５では、データ蓄積部１３からのデータに対してＩＰパケット化、メディアアクセス制御（Media Access Control、ＭＡＣ）フレーム化、ＭＰＥＧ（Moving Picture Experts Group Phase）２のトランスポート化などのフォーマット変換を行う。また、データ作成部１５は、データのＩＰパケット化後と、トランスポート化後に、上記２重の暗号化を行う。

【００２８】このフォーマット変換について以下に説明する。上述したように、近年、オーディオ、ビデオ信号やデータのような多種類のデータが多重化されて、大容量のディジタル回線で伝送されることが可能になってきた。この多重化の方法としては、例えばＭＰＥＧ２の伝送フォーマットであるトランスポートストリーム（Transport Stream，ＴＳ）パケットが知られている。このＴＳパケットでは、情報データ部（ペイロード部）に暗号化処理を施している。この暗号化のための暗号化鍵は、ＴＳパケットのヘッダ部分の１３ビットのパケットＩＤ（ＰＩＤ）及び２ビットのスクランブル制御部に対応した固有のビット列を使用する。また、上記ＰＩＤは、各ＴＳパケットの特定チャンネルのビデオやオーディオ等の情報種類を識別するのにも使われる。

【００２９】このＴＳパケットを用いてデータを伝送する場合には、データをインターネットで広く使用されているインターネットプロトコル（ＩＰ）パケットのフォーマットに変換し、さらにこのＩＰパケットをＴＳパケットに入れ込んでいる。

【００３０】ところで、多種類のデータがＩＰパケットとして伝送される場合、上記ＰＩＤはＩＰパケットのデータを他のビデオやオーディオのデータと識別するために使われており、又ビット長も１３ビットしか無く、ＩＰパケットで伝送される種々のデータの種別を識別させるには不十分なビット数である。そこでＰＩＤ以外のデータ種類の識別方法が必要になる。

【００３１】例えば、インターネット上では受信データが自分宛のデータであるか否かを識別するのにＩＰパケットのＩＰヘッダに含まれる送信先アドレス（DestinationAddress）を用いている。ＴＳパケットでＩＰパケットを伝送する場合でも、この送信先アドレス（以後、送信先ＩＰアドレスという。）を用いて自分宛のデータであるかを識別することが可能である。

【００３２】しかし、例えば衛星回線を例にとるとデータ伝送速度が１中継器当たり３０Ｍｂｐｓとなり、データ受信側でリアルタイムに送信先ＩＰアドレスの解析をソフトウェアで行うことは非常に困難である。何らかの手段により、自分宛の情報だけを抽出する手段が必要となる。

【００３３】さらに、具体的な情報のタイトルを指定しなくとも、自分の関心のある情報のジャンルの情報だけ指定しておけば、そのジャンルの情報だけが自動的に受信され、ダウンロードできると大変便利である。

【００３４】又、特定の加入者だけに受信可能とするために、上述したようにデータを暗号化した場合、受信側では暗号化されたデータを復号する必要がある。

【００３５】そこで、上記データ伝送システムでは、データ配信装置１０において複数種類のデータブロックからなる多重化データにデータの種類を示す識別子を付加し、通信衛星１８を経由させて上記衛星回線により、データ受信装置３０に送信している。そして、データ受信装置３０では、ハードウェア的に上記識別子を読み取り、受信者が必要とする予め登録された種別のデータのみを抽出して復号する。

【００３６】この識別子の付加は、データ配信装置１０のデータ作成部１５によって行われる。データ配信装置１０内のデータ蓄積部１３には、ユーザが必要とするデータが何も加工されていない状態で蓄積されている。データ管理部１２から、データの読み出し要求がユーザから来たことを知らされたデータ蓄積部１３は、リクエストされたデータ及びユーザの宛先情報を同時にデータ作成部１５に高速スイッチャ１４を介して送る。

【００３７】ここで、ユーザの宛先情報とは、ＩＰパケット送信に必要な送信先ＩＰアドレスである。このデータ伝送システムでは、すべてのユーザに固有の送信先ＩＰアドレスを割り振っている。一のユーザが持つ送信先ＩＰアドレスは、一のユーザが確保している間は、一のユーザ以外のユーザは持たない。

【００３８】データ蓄積部１３からのデータは、データ

作成部１５によって作成又はフォーマット変換された後、データ処理部１６で他のオーディオ信号やビデオ信号と多重化され、多重化データとして送信アンテナ１７から通信衛星１８に無線回線を介して送られる。

【００３９】通信衛星１８を介して送られた多重化データは、特定ユーザの所有するデータ受信装置３０に限らず、データを受信できる状況にある全てのユーザが受信することが可能である。データ受信装置３０は、通信衛星１８からの全多重化データを受信し、その中から、自分が出したリクエストに応じたデータを選別して抽出し、復号化する。

【００４０】このデータ受信装置３０は、データの種類を示す識別子が付加された複数種類のデータブロックよりなる多重化データを通信衛星１８による衛星回線を介して受信し、上記識別子を読み取ることにより、予め登録された種類のデータブロックのみを抽出して復号する。

【００４１】すなわち、データ受信装置３０は、リクエストに応じて送信されたデータを含む多数のデータブロックを受信し、その中から、自分宛のデータブロック、自分が受け取るべきデータブロック、自分が受け取ることができるデータブロックを選別して抽出する。なお、予めユーザとデータ提供者との契約によって、ユーザが持つデータ受信装置３０は決定されている。

【００４２】したがって、通常であれば、ユーザが持つデータ受信装置３０を用いて、他のユーザ宛の特有のデータを選別することができない。

【００４３】しかし、通信衛星１８を用いる上記データ伝送システムでは、電話回線、専用回線などの１対１通信と異なり、不特定多数の受信者が受信装置で容易に受信できるので、盗聴されやすい。すなわち、データ伝送が盗聴される可能性が高い。そこで、上記データ伝送システムでも、データの暗号化が必要とされる。

【００４４】このため、データ配信装置１０は、図２に簡単に示すように、情報を提供するコンテンツプロバイダ１８と、その情報を伝送するサービスプロバイダ１９とで、暗号化器２１と、暗号化器２６により２重の暗号化処理を施している。

【００４５】このデータ配信装置１０は、実際には、上述した図１に示すように構成されており、特に図２に示したコンテンツプロバイダ１８と、サービスプロバイダ１９の備える各部は、図３に示すようなデータ作成部１５に含まれる。

【００４６】データ蓄積部１３から送られてきた特定ユーザ宛のデータ及びＩＰアドレスは送信先ＩＰパケット作成部２０に送られる。ＩＰパケット作成部２０では、データ蓄積部１３から送られてきたデータとその時点でユーザを特定する送信先ＩＰアドレスを用いて、図４に示すＩＰパケット６０を生成する。このＩＰパケット６０の大きさはＴＣＰ／ＩＰ（Transmission Control Protocol／Internet Protocol）で規定され、ユーザがリクエストしたデータがその大きさを超える場合には、このデータは複数のＩＰパケットに分割されて次の暗号化器２１に転送される。

【００４７】ここで使用されるＩＰパケット６０のＩＰヘッダには、図５に示すユーザの送信先ＩＰアドレス７４と、送信元のＩＰアドレス７３が入っている。ここで、送信先ＩＰアドレス７４は、３２ビットである。

【００４８】ＩＰパケット作成部２０で作成されたＩＰパケット６０は、暗号化器２１に転送される。暗号化器２１では、ＩＰパケット６０内の３２ビットの上記送信先ＩＰアドレス７４によって、宛先が特定のユーザであることを知り、その時点で既にデータ提供者と特定のユーザとの間のみで知り合うＩＰパケット用暗号化鍵によってＩＰパケット６０全体を暗号化する。暗号化式としては、例えばＤＥＳ（Data Encryption Standard）などが採用される。

【００４９】この暗号化器２１は、上記３２ビットの送信先ＩＰアドレス７４を用いた暗号化を行うので、ＩＰパケットの暗号化による限定受信だけでも２の３２乗（＝約４３億）個の範囲に受信者を分けることができる。

【００５０】ここで、コンテンツプロバイダ１８は、データ受信装置３０に対して、伝送するＩＰパケットの送信先ＩＰアドレスと、暗号化ＩＰパケットを復号するための復号鍵を予め与えておく。そして、ＩＰパケットのペイロード部分をこの復号鍵に対応する暗号鍵で暗号化し、サービスプロバイダ１９に送る。

【００５１】ただし、暗号化は、特定のユーザに対する全てのデータについて施す必要はなく、データの種類によっては暗号化が行われないこともある。暗号化が行われない場合には、ＩＰパケット作成部２０からＭＡＣフレーム作成部２２に直接ＩＰパケット６０が転送される。

【００５２】ここでは、暗号化が行われる場合について説明する。暗号化は通常６４ビットの平文に対して行われ、暗号化すべきＩＰパケット６０のデータ長が６４ビットの倍数でない場合には、データの埋め合わせ、すなわち無効データのパディングを行うことでＩＰパケット６０全体を６４ビットの倍数にし、ＩＰパケット６１とする。

【００５３】特定のユーザ用のＩＰパケット６１が暗号化されたＩＰパケット６２は、ＭＡＣフレーム作成部２２に転送される。ＭＡＣフレーム作成部２２では、暗号化器２１によって暗号化されたＩＰパケット６２に対して、ＭＡＣヘッダ７０を付加する。

【００５４】このＭＡＣヘッダ７０は、図６に示すように８ビットのＳＳＩＤ（Server System ID）と、２４ビットのＵＤＢ（User Depend Block）１と、３２ビットのＵＤＢ２の計６４ビットで構成されている。特に、Ｍ

ＡＣヘッダ７０のＵＤＢ２には、上記ＩＰヘッダ内に書かれた送信先ＩＰアドレスと同様の送信先ＩＰアドレスが書き込まれる。

【００５５】上記ＩＰヘッダ内の送信先ＩＰアドレスは暗号化されており、受信装置側では暗号を復号しなければ送信先ＩＰアドレスを知ることができないが、上記ＭＡＣヘッダ７０にそれと同じ送信先ＩＰアドレスがあれば、受信側では単にハードウェア的にそれを読み出すことで、自分宛のデータブロックであるか否かを知ることができる。この送信先ＩＰアドレスはＩＰパケット作成部２０からＭＡＣフレーム作成部２２に直接渡される。

【００５６】なお、上記ＵＤＢ１には、３ビットのＰＢＬ（Padding_Byte_Length）と、１ビットのＣＰ（Control_Packet）と、１ビットのＥＮ（Encrypted_or_Not）と、１ビットのＰＮ（Protocol_Type Available_or_Not）と、２ビットのReserveと、１６ビットのプロトコル番号（Protocol Type）がセットされる。

【００５７】この内、ＰＢＬは、パディングバイト長であり、暗号化の際に埋め合わせされた無効なデータの長さである。これは、暗号化されたＩＰパケットを受信したユーザが正規なデータ長を知るために必要となる。

【００５８】また、ＣＰは、ＩＰパケットに、ユーザが必要なデータかシステム運用に必要な制御データが入っているかを識別するビットである。通常、ユーザがリクエストした際に受け取るべきＭＡＣフレーム６３のＣＰは、制御データではなくデータが入っていることを示している。

【００５９】ＥＮは、ＩＰパケットが暗号化器２１によって暗号化されているか否かを示す制御ビットである。このビット情報によってユーザは受信したＭＡＣフレーム６３を復号するかしないか決定する。ＰＮは、Protocol Typeエリアに有用な情報があるか否かを示す制御ビットである。

【００６０】図３のＭＡＣフレーム作成部２２では、以上の制御ビットをＩＰパケット６２に付加している。ここで、ＵＤＢ２には、上記送信先ＩＰアドレスの他、ＩＰパケットの情報の種類を表すコンテンツＩＤをセットしてもよい。このコンテンツＩＤについては後述する。ＵＤＢ２にセットされたのが、上記送信先ＩＰアドレスであるか上記コンテンツＩＤであるかを識別させるのが上記ＳＳＩＤである。

【００６１】ＭＡＣフレーム作成部２２で生成されたＭＡＣフレーム６３には、ＣＲＣ計算部２３にて計算されたＣＲＣ（Cyclic Redundancy Checking、巡回冗長検査）が付加される。このようにデータ配信装置１０側でＣＲＣの計算を行うことで、データ受信装置３０は、受信したＭＡＣフレームが正しく通信衛星１８から伝送されているかを検査することができる。ＣＲＣ計算部２３において生成された１６ビットのＣＲＣは、ＭＡＣフレーム６３の最後に付加されている。

【００６２】このＭＡＣフレーム６３は、セクション作成部２４に転送されてＭＰＥＧ２で規定されるセクションに変換される。図４に示すように、ＭＡＣフレーム６３は、セクション（Ｓｅｃ）ヘッダ７１の直後に付加され、プライベートセクション６４と呼ばれる。

【００６３】このセクションヘッダ７１のフォーマットを図７（Ａ）に示す。セクションヘッダ７１のフォーマットは、ＭＰＥＧ２によって、規定され、テーブル（ＩＤ）T_{id}、セクションーシンクーインディケータS_{si}、プライベートーインディケータP_i、リザーブドR_{es}、プライベートーセクションーレングスP_{sl}を有する。ここで、プライベートーセクションーレングスP_{sl}には、ＭＡＣフレームのデータ長が入る。

【００６４】セクション作成部２４で作成されたプライベートセクション６４は、トランスポートパケット作成部２５に転送される。トランスポートパケット作成部２５では、転送されたプライベートセクション６４をトランスポートパケット65_1，65_2，・・65_nに分割する。

【００６５】トランスポートパケット65_1，65_2，・・65_nは、それぞれ１８８バイトで構成されている。これらのトランスポートパケット65_1，65_2，・・65_nには、４バイトのＴＳヘッダが付加される。

【００６６】例えばＴＳヘッダ７２のフォーマットを図７（Ｂ）に示す。ＴＳヘッダ７２は、シンクバイトS_{yb}、トランスポートーエラーーインディケータT_{ei}、ペイロードーユニットースタートーインディケータP_{ui}、トランスポートープライオリティT_p、上記ＰＩＤ、上記スクランブル制御部（トランスポートースクランブルーコントロール）T_{sc}、アダプティションーフィールドーコントロールA_{fc}及びコンティニティーカウンタC_cを有する。

【００６７】トランスポートパケット65_1，65_2，・・65_nの１個分の大きさは、上述したように１８８バイトと規定されているので、一般的に、一つのセクション６４を複数のトランスポートパケットに分割する必要がある。

【００６８】ここで、通常、一つのセクションは１８４バイト（１８８バイトからヘッダ長の４バイトを引いたバイト数）の整数倍長とは限らないので、一つのセクション６４を複数のトランスポートパケット65_1，65_2，・・65_nに分割する際には、図４に示すように、スタッフィングバイトを用いたデータの穴埋めを行う。すなわち、１８４バイトの倍数でない一つのセクションを複数のトランスポートパケットに分割した場合、最後のトランスポートパケットの余ったデータエリアに、全てのビットがスタッフィングされたスタッフィング領域を形成する。

【００６９】トランスポートパケット作成部２５で作成された各トランスポートパケットは、暗号化器２６に供

給される。暗号化器２６は、図２に示すようにＴＳパケット用暗号化鍵を用いて、上記各トランスポートパケットのデータ部分に暗号化処理を施す。

【００７０】サービスプロバイダ１９は、データ受信装置３０に対して、伝送するＴＳパケットのＰＩＤ部分とスクランブル制御部の値と、このＴＳパケットを復号する復号鍵を予め与えておく。そして、コンテンツプラバイダ１８から与えられた暗号化ＩＰパケットをＴＳパケット化し、さらにこのＴＳパケットのペイロード部分を上記復号鍵に対応する暗号鍵で暗号化して、暗号化ＴＳパケットを作成し、衛星回線上に送信する。

【００７１】ここで、暗号化のための暗号化鍵は、上述したように、図７の（ｂ）に示したＴＳヘッダのＰＩＤ（１３ビット）とスクランブル制御部（２ビット）に対応した固有のビット列を使用する。このため、最大で１５ビット分、４０９６通りの限定ができる。

【００７２】既にＩＰパケットの送信先ＩＰアドレスを用いて上述したように２の３２乗個の範囲に受信者を分けることができているので、このＴＳパケットの暗号化を組み合わせると、さらにその４０９６倍の範囲に受信者を分けることができ、より細やかな限定受信方式を構成できる。

【００７３】また、独立の暗号化を２重に行うことにより、盗聴者がいずれか一方の暗号を解読することに成功したとしても、もう一方の暗号を解読できなければ平文データを得ることはできないので、より安全性の高い限定受信方式を構成できる。

【００７４】また、ここではＩＰパケットの暗号化による限定受信方式と、ＴＳパケットの暗号化による限定受信方式をそれぞれコンテンツプロバイダ１８と、サービスプロバイダ１９という別の事業者で行うので、他者とは独立の限定受信方式を構成できる。これは、伝送路を提供する事業者と、伝送データを提供する事業者が異なり、それぞれが独立にユーザと限定受信契約を結びたい場合に有効である。事業者間で暗号鍵に関する情報が漏れてしまう虞もない。

【００７５】コンテンツプロバイダ１８と、サービスプロバイダ１９で２重の暗号化が施されたデータは、データ転送部２７に転送された後、マルチプレクサ等のデータ処理部１６に伝送される。データ処理部１６では、上記トランスポートパケットを他のディジタル化されたビデオ、オーディオ信号と多重化した後、変調、増幅する。

【００７６】ブロードキャストされた特定ユーザのためのデータは、ユーザ側の受信アンテナ３１で受信され、特定のユーザのデータ受信装置３０に転送される。

【００７７】受信アンテナ３１により受信された信号は、ＩＦの信号に変換され、データ受信装置３０に入力される。図８にこのデータ受信装置３０のブロック図を示す。また、図９には、このデータ受信装置３０で行われる２重の復号処理のフローチャートを示す。

【００７８】チューナ３３，Ａ／Ｄ変換器３４，復調器３５及びデコーダ３６からなるフロントエンド３２に入力された信号は、ここでディジタル信号に変換され、ＱＰＳＫ復調処理及び誤り訂正処理が施されて、ステップＳ１のように暗号化されたＴＳパケットデータとして受信される。

【００７９】この暗号化されたＴＳパケットは、デスクランブラ３７に供給される。デスクランブラ３７は、上記暗号化されたＴＳパケットデータにＴＳパケットレベルのデスクランブル処理を施す。この場合、デスクランブラ３７は、上記暗号化ＴＳパケットデータのヘッダ部分からＰＩＤ部とスクランブル制御部の値を読みとり、この値に対応するＴＳパケット用復号鍵がサービスプロバイダ１９から与えられているか否かをステップＳ２で判断し、与えられているならばステップＳ３でこの暗号化ＴＳパケットのペイロード部分をこの復号鍵により復号し、復号されたＴＳパケットを出力する。ここで、復号鍵がサービスプロバイダ１９から予め与えられていなければ、ステップＳ７で暗号化ＴＳパケットを破棄する。

【００８０】ステップＳ３で復号されたＴＳパケットは、デマルチプレクサ３８に供給される。ここで、デマルプレクサ３８は、上記データ処理部１６で上記ＴＳパケットデータと共に多重化されたオーディオデータとビデオデータを分割し、オーディオデータをオーディオデコーダ３９に供給し、ビデオデータをビデオデコーダ４０に供給する。オーディオデコーダ３９は、アナログオーディオを出力し、ビデオーデコーダ４０はＮＴＳＣエンコーダ４１を介してアナログビデオを出力する。残ったＴＳパケットデータは、デパケタイザ４５に供給される。

【００８１】デパケタイザ４５は、図４で示したプライベートセクション６４のフォーマットを再生し、ＣＲＣの値を計算し、データが正しく受信されたか否かを判定する。そして、デパケタイザ４５は、ステップＳ４で上記プライベートセクション６４をＩＰパケット化し、図１０に示すようなフォーマットデータ７５に変換する。このフォーマットデータ７５は、ＦＩＦＯ４６を介してこのＩＰパケットを復号する復号器４７に転送される。

【００８２】復号器４７では、フォーマットデータ７５内のＭＡＣヘッダの図６に示したＵＤＢ２にセットされた識別子、ここでは送信先ＩＰアドレスを取り出し、これに対応するＩＰパケット用復号鍵がコンテンツプラバイダ１８から与えられているか否かをステップＳ５で判断し、与えられていれば、ステップＳ６でＩＰパケットのペイロード部分をこの復号鍵を用いて復号し、復号されたＩＰパケットを出力する。ここで、復号鍵がコンテンツプロバイダ１８から予め与えられていなければ、ステップＳ７で暗号化ＩＰパケットを破棄する。

【００８３】復号鍵は、上記識別子に対応させて、デュアルポートラム（ＤＰＲＡＭ）４８内の図１１に示す参照テーブル８０に収納されている。

【００８４】この参照テーブル８０は、受信可能な種類のデータブロックの識別子をその識別子と対応する復号鍵と共に持っている。識別子としては４バイトを使っており、復号鍵としては８バイトを使っている。

【００８５】図中、識別子としては上述したように、送信先ＩＰアドレスを用いても、コンテンツＩＤを用いて良く、その識別は受信パケットのＭＡＣヘッダの中のＳＳＩＤで行う。又参照テーブル８０の値の設定はＤＰＲＡＭ４８への入力を持つＣＰＵ４２により行われる。

【００８６】復号器４７は、上記図１０のフォーマットで暗号化ＩＰパケットデータを受信し、ＭＡＣアドレス内のＵＤＢ２の識別子を取り出すと、ＤＰＲＡＭ４８にアクセスし、先頭のアドレスから１６バイトおきにテーブル８０中の識別子を検索し、識別子の後の４バイトに格納されたマスクビットの内、“１”となっている識別子のビットに対して受信パケット中の識別子とテーブル中の識別子の一致検出を行う。

【００８７】マスクビットがＨ“ｆｆｆｆｆｆｆｆ”となっていれば、受信したパケットのＭＡＣアドレス中の識別子とテーブル中の識別子の全ビットの一致を確認し、入力した識別子と同じ識別子がＤＰＲＡＭ４８内にあるとし、その識別子に対応する復号鍵（図中セッションキー）を取り出し、それ以降のＩＰパケットの復号処理を行う。

【００８８】予め登録された参照テーブル８０中の識別子の最後には、ＥＮＤコードがストアされており、識別子を検索していき、ＥＮＤコードが検出された場合は、そこで検索を抜け出し、その受信パケットは受信せずにステップＳ７で示したようにこの復号器４７で廃棄される。

【００８９】識別子としては、上述したように、送信先ＩＰアドレスの他、コンテンツＩＤ（またはジャンルＩＤ）を使う。すなわち、図６に示したＭＡＣヘッダ７０のＵＤＢ２には、送信先ＩＰアドレスの他、コンテンツＩＤがセットされてもよい。ＳＳＩＤとして例えば“０”がセットされている場合には、送信先ＩＰアドレスを用いることを示し、例えば“１”がセットされている場合には、ジャンルＩＤを用いることを規定する。ＳＳＩＤを受信側で解析することによりどちらが使われているかを判別できる。

【００９０】例えば、ＵＤＢ２に送信先ＩＰアドレスを用いた場合、ユニキャストアドレスに対応する個人宛、及びマルチキャストアドレスを用いてグループのユーザ宛のデータを伝送することが可能となり、受信側では自分宛かあるいは自分が所属しえいるグループ宛のデータのみリアルタイムで受信することが可能となる。

【００９１】この場合、データ受信装置３０のＤＰＲＡＭ４８は図１２に示すようなフォーマットの参照テーブル８１を備えていればよい。この参照テーブル８１は、受信可能な種類のデータブロックの送信先ＩＰアドレスをその送信先ＩＰアドレスと対応する復号鍵と共に持っている。例えば、始めの１６バイトには上記マルチキャストアドレスのようなグループ用の送信先ＩＰアドレス１がセットされている。

【００９２】この送信先ＩＰアドレス１の暗号化ON／OFFフラグは０である。また、次の１６バイトには上記ユニキャストアドレスのような個人宛の送信先ＩＰアドレス２がセットされている。暗号化ON／OFFフラグは１である。送信先ＩＰアドレス２にもセッションキーがセットされている。

【００９３】復号器４７は、上記図１０のフォーマットでＩＰパケットデータを受信し、ＭＡＣアドレス内の送信先ＩＰアドレスを入力すると、ＤＰＲＡＭ４８にアクセスし、先頭のアドレスから１６バイトおきにテーブル８１中の送信先ＩＰアドレスを検索し、該ＩＰアドレスの後の４バイトに格納されたマスクビットの内、“１”となっている識別子のビットに対して受信パケット中の識別子とテーブル中の識別子の一致検出を行う。

【００９４】マスクビットがＨ“ｆｆｆｆｆｆｆｆ”となっていれば、受信したパケットのＭＡＣアドレス中の送信先ＩＰアドレスとテーブル中の送信先ＩＰアドレスの全ビットの一致を確認し、入力したＩＰアドレスと同じＩＰアドレスがＤＰＲＡＭ４８内にあるとし、そのＩＰアドレスに対応する復号鍵を取り出し、それ以降のＩＰパケットの復号処理を行う。

【００９５】予め登録された参照テーブル８１中のＩＰアドレスの最後には、ＥＮＤコードがストアされており、ＩＰアドレスを検索していき、ＥＮＤコードが検出された場合は、そこで検索を抜け出し、その受信パケットは受信せずにこの復号器４７でステップＳ７のように廃棄される。

【００９６】一方、ＵＤＢ２として３２ビットをフルに使ったコンテンツＩＤを用いる場合は、予め登録しておいたジャンルのデータが受信された場合にデータをＰＣに転送し、ハードディスクに自動的にダウンロードすることが可能となる。

【００９７】この場合、データ受信装置３０のＤＰＲＡＭ４８は図１３に示すようなフォーマットの参照テーブル８２を備えていればよい。この参照テーブル８２は、受信可能な種類のデータブロックの例えばコンテンツＩＤ８３を３２ビットフルに使って、記憶している。

【００９８】このような３２ビットのコンテンツＩＤ８３は、図１４の（Ａ）に示すように、８ビットの大分類D_0と、６ビットの中分類D_1と、４ビットの小分類D_2と、１４ビットの情報ＩＤとによって構成されている。大分類D_0は、コンピュータソフト、出版物、ゲームソフトというような大きなカテゴリーを表す。中分類D_1

は大分類D_0が出版物であれば、書籍、雑誌、新聞というような中間のカテゴリーを示す。さらに、小分類D_2は中分類D_1が新聞であれば、Ａ新聞、Ｂ新聞、Ｓ新聞という新聞社名を表すカテゴリーを示す。そして、この小分類D_2の中の唯一のＩＤにより一つのデータ単位が識別される。この場合、新聞の発行の日付が情報ＩＤとなり、結果的に例えば図１４の（Ｂ）に示すようなコンテンツＩＤとなる。

【００９９】このようなコンテンツＩＤを識別子として用いた場合の実際の情報識別の方法を以下に述べる。例えば、上記図１４の例では、Ａ新聞を契約する場合は、マスクビットをＨ“ｆｆｆｆｃ０００”としてこのマスクビットが１のビット位置の受信パケットの識別子とテーブル中の識別子の一致を検出すればよい。また、固有の新聞名によらず、全ての新聞を受信する場合は、マスクビットをＨ“ｆｆｆｃ００００”としておけば、Ａ新聞Ｈ“０２０８４０００＋発行日ＩＤ”、Ｂ新聞Ｈ“０２０８８０００＋発行日ＩＤ”も全て一つの設定でダウンロードすることができる。

【０１００】これは、いちいち個々の情報のＩＤを指定しなくても、必要な情報のジャンルだけ指定しておけば、自動的に指定したジャンルの情報が受信できる、という点で、大変有用な方法である。

【０１０１】ただこの場合、例えば各新聞が別々のセッションキーで暗号化されているように、各情報が暗号化されている場合は、コンテンツＩＤを設定するだけでは、各新聞に対するセッションキーを設定できないため、あくまでも各情報が暗号化されていない場合に有効な方法である。

【０１０２】なお、上記情報の識別子としては、４８ビット長で各製品に割り当てられているＭＡＣアドレスを用いる方法もある。

【０１０３】復号器４７で、送信先ＩＰアドレスや、コンテンツＩＤを読むことが出来れば、このデータブロックが予め登録された種類のデータブロックであると判断して抽出し、フォーマットデータ７５内の暗号化されたＩＰヘッダとＩＰデータを上述したように復号する。

【０１０４】復号化されたデータブロックは、パーソナルコンピュータ上のメインメモリにＦＩＦＯ４９及びＰＣＩインターフェース５０を介して転送される。そして、このパーソナルコンピュータのソフトウェアによる処理がなされる。

【０１０５】ＣＰＵ４２は、ＤＰＲＡＭ４８の読み出しを制御すると共に、参照テーブルの値の設定を行う。また、ＣＰＵ４２は、ＲＯＭ４４からＲＡＭ４３に読み込まれたプログラムにしたがって、デマルチプレクサ３８、ＤＰＲＡＭ４８、ＤＰＲＡＭ５２を制御する。また、ＣＰＵ４２は、ＩＣカードリーダ５３から読み込んだデータを処理し、上記復号鍵を生成してもよい。また、上記リクエストをモデム５４、及び電話回線５６を介してＩＳＤＮによりデータ供給元に送信する。

【０１０６】以上説明したように、このデータ受信装置３０は、データ配信装置１０によりＭＡＣフレームのＤＢＵ２にセットされて伝送されてきた、送信先ＩＰアドレスや、コンテンツＩＤを復号器４７により読み取り、予め登録された種類のデータブロックのみを抽出することができるので、種々の暗号化されたデータが多重化された受信データの中から高速に、自分宛あるいは必要とする情報だけを抽出して復号できる。

【０１０７】また、伝送されたデータは、図２に示したように、コンテンツプロバイダ１８、サービスプロバイダ１９で２重に暗号化されており、データ受信装置３０のみが、それを復号化する二つの復号鍵を持っていることから、データが他人に盗用されることを防止できる。

【０１０８】なお、この実施の形態となるデータ伝送システムは、データ配信装置１０側の２重暗号化処理を図１５に示すような構成で行ってもよい。すなわち、ＩＰパケットの暗号化処理をコンテンツプロバイダ１８に行わせるのではなく、サービスプロバイダ１９に行わせる。このため、コンテンツプロバイダ１８は、経費を節約できる。

【０１０９】すなわち、一つの事業者が両方の暗号化処理を行うように構成すれば、もう一方の事業者は暗号化処理のための設備を持つ必要がなくなる。これは、例えば一つのサービスプロバイダの提供する伝送路を複数のコンテンツプロバイダが利用する場合に、それぞれのコンテンツプロバイダが暗号化処理設備を持たなくてよいので有効である。

【０１１０】ここで各部の動作は、図２に示した各部の動作と同様であり、またデータ受信装置３０の構成も同様であるので説明を省略する。

【０１１１】また、データ受信装置３０内の構成を図１６に示すようにしてもよい。すなわち、デパケタイザ４５と復号器４７との間に例えばハードディスクドライバのような記憶装置５８を設け、暗号化されたＩＰパケットを蓄積しておく構成としてもよい。このようにすれば、予めＩＰパケットを復号する復号鍵を得ていなくても、暗号化されたＩＰパケットを記憶装置５８に蓄積しておいて、後から上記復号鍵を得た時点で復号すればよい。

【０１１２】すなわち、暗号化されたパケットを記憶装置に保存しておくようにすることにより、受信装置が復号鍵を後から得てもデータが有効となるようにできる。例えば、予め大量のデータを記憶装置に保存しておき、ユーザが意図した段階で復号鍵を得てデータを利用することにより、ユーザが意図してからデータを受信し始めるのに比べて、大量のデータを受信するための時間が節約できる。

【０１１３】ここでは、受信装置３０がＩＰパケットを復号するための復号鍵を得ていない場合を説明したが、

ＴＳパケットを復号するための復号鍵を得ていない場合でも、暗号化されたままのＴＳパケットを記憶装置に保存しておくことにより同様の処理を行える。

【０１１４】さらに、暗号化されたデータは、保存できるが、復号されたデータや復号鍵は保存できないような仕組みを付け加えることにより、平文データがコピーされることを防ぐことも可能になる。

【０１１５】また、上述した各例では、伝送データとしてＩＰパケットを考えたが、同様の構造を持つ他の伝送プロトコルパケットを考えても、同様の限定受信方式が構成可能である。また、伝送データのパケット化を３重以上として、３つ以上の限定受信方式を組み合わせてもよい。このため、ＩＰパケット化前のファイルデータに暗号化処理を施しておいてもよい。

【０１１６】また、例えば、ＭＡＣフレームのデータ圧縮方法は、ＭＰＥＧ２には限定されず、他の圧縮方法を用いてよい。また、インターネットプロトコルは、ＴＣＰ／ＩＰには限定されず、例えばＯＳＩ（Open System Interconnection）方式を用いてもよい。

【０１１７】

【発明の効果】本発明に係る情報伝送装置及び方法は、上記ディジタルデータに上記ディジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含めた少なくとも２重の暗号化処理を施してからこの暗号化データを送信し、データ伝送路を介して受信した上記暗号化データにそれぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施すので、通信衛星を用いてディジタルデータを伝送する際にも、情報の漏洩の度合い、妨害の度合いを低くできる。

【０１１８】また、本発明に係る情報受信装置及び方法は、データの種類を示す識別子が付加された複数種類のデータブロックをデータ伝送路を介して受信し、上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号するので、情報配信者からデータ伝送路を介して伝送されたディジタルデータを、高速にデータの種類に応じて特定のユーザに受信させることができる。

【０１１９】また、本発明に係る情報記憶媒体は、ディジタルデータの種類を示す識別子に応じた暗号鍵による暗号化処理が少なくとも施された暗号化データを記憶しているので、受信装置が復号鍵を後から得てもデータを有効に利用できる。

【０１２０】さらに、本発明に係る情報記憶媒体は、データブロックの種類を示すコンテンツＩＤが付加された複数種類のデータブロックを記憶するので、必要とする情報だけを簡単に抽出することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態となるデータ伝送システムの構成図である。

【図２】上記データ伝送システムの２重暗号化処理に関わる構成を簡単に示したブロック図である。

【図３】上記図１に示したデータ作成部の構成を示すブロック図である。

【図４】上記図３に示したデータ作成部でのデータ作成の過程を説明するための図である。

【図５】ＩＰヘッダの詳細な構成を示すフォーマット図である。

【図６】ＭＡＣヘッダのフォーマット図である。

【図７】セクションヘッダとＴＳヘッダのフォーマット図である。

【図８】上記データ伝送システムを構成するデータ受信装置のブロック図である。

【図９】上記データ受信装置で行う復号化処理を説明するためのフローチャートである。

【図１０】上記データ受信装置内のデパケタイザから復号器へのデータの転送を説明するための図である。

【図１１】上記データ受信装置内のＤＰＲＡＭが格納する参照テーブルの基本的な構成図である。

【図１２】上記参照テーブルの第１の具体例を示す図である。

【図１３】上記参照テーブルの第２の具体例を示す図である。

【図１４】コンテンツＩＤの具体的構成例を示す図である。

【図１５】上記データ伝送システム内のデータ配信装置の他の具体例を示すブロック図である。

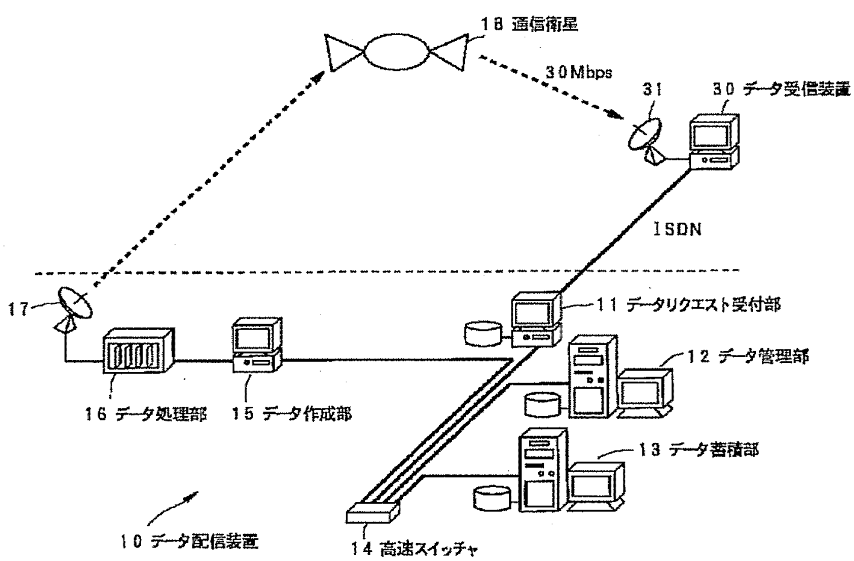
【図１６】上記データ伝送システム内のデータ受信装置の他の具体例を示すブロック図である。

【図１７】伝送路上のデータを共通鍵暗号方式で暗号化する暗号化データ伝送装置の一例を示す概略構成図である。

【符号の説明】

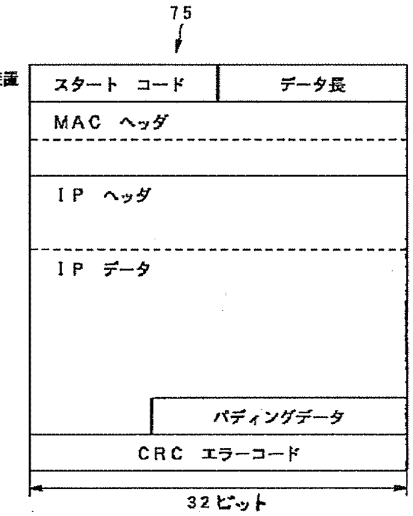
１０　データ配信装置、１８　コンテンツプロバイダ、１９　サービスプロバイダ、２１　暗号化器、２５　ＴＳパケット作成部、２６　暗号化器、３０　データ受信装置、３７　デスクランブラ、４５　デパケタイザ、４７　復号器

【図１】



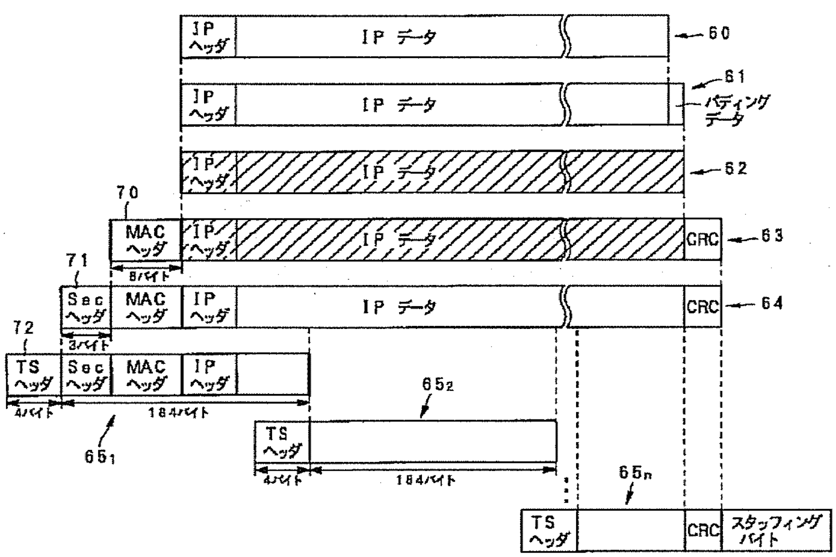
18 通信衛星
30Mbps
31
30 データ受信装置
ISDN
17
11 データリクエスト受付部
12 データ管理部
13 データ蓄積部
16 データ処理部
15 データ作成部
10 データ配信装置
14 高速スイッチャ

【図１０】



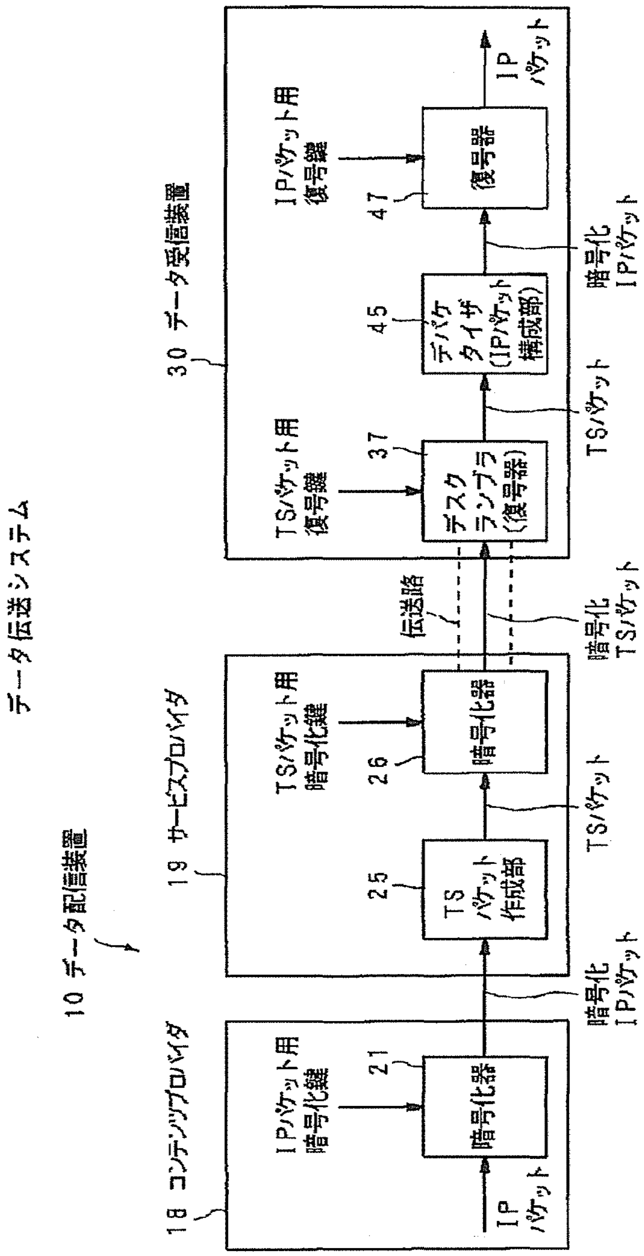
75
スタート コード
データ長
MAC ヘッダ
IP ヘッダ
IP データ
パディングデータ
CRC エラーコード
32ビット

【図４】

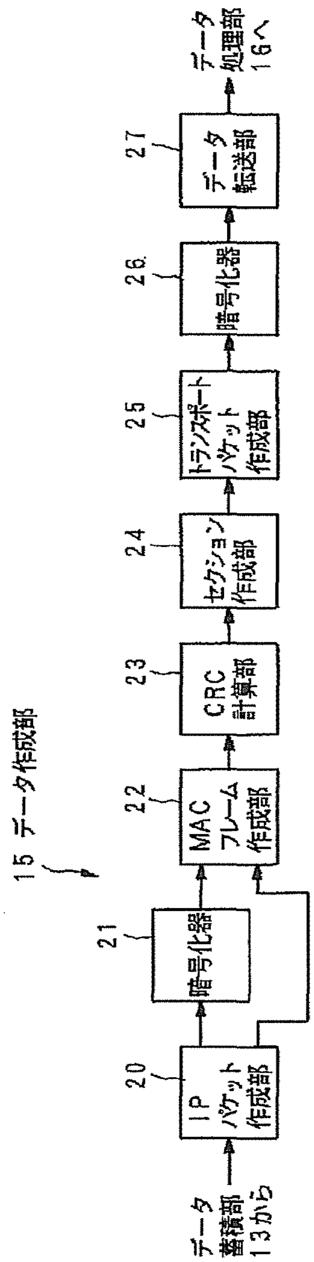


IP ヘッダ
IP データ
60
61
パディング データ
62
70
MAC ヘッダ
CRC
63
8バイト
71
Sec ヘッダ
64
3バイト
72
TS ヘッダ
4バイト
184バイト
65_1
65_2
65_n
スタッフィング バイト

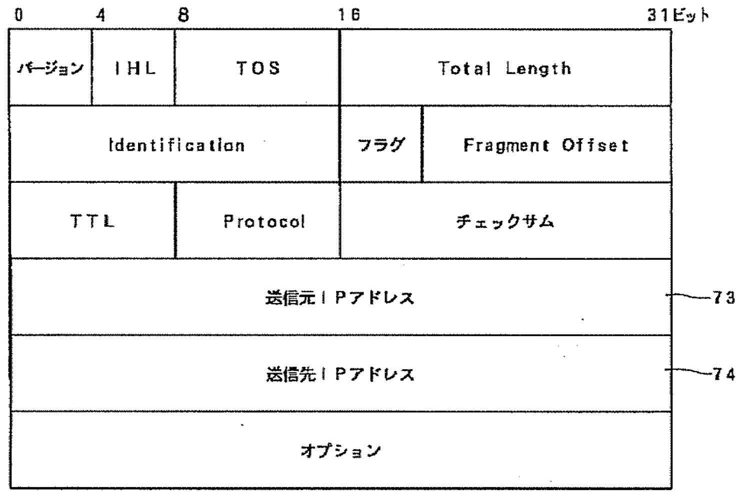
【図２】


データ伝送システム
10 データ配信装置
18 コンテンツプロバイダ
IPパケット用暗号化鍵
21
暗号化器
IPパケット
暗号化IPパケット
19 サービスプロバイダ
25
TSパケット作成部
TSパケット
TSパケット用暗号化鍵
26
暗号化器
暗号化TSパケット
伝送路
30 データ受信装置
TSパケット用復号鍵
37
デスクランブラ(復号器)
TSパケット
45
デパケタイザ(IPパケット構成部)
暗号化IPパケット
IPパケット用復号鍵
47
復号器
IPパケット

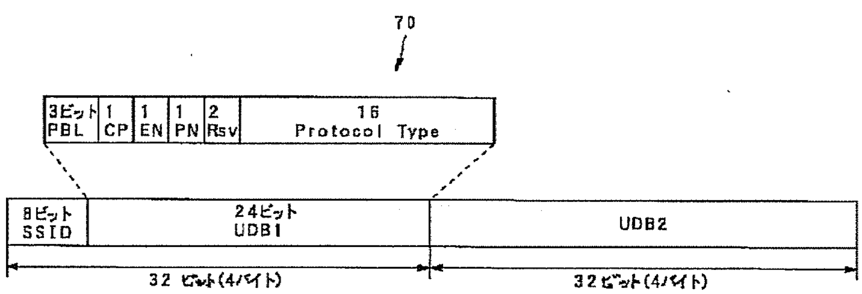
【図３】


15 データ作成部
データ蓄積部13から
20
IPパケット作成部
21
暗号化器
22
MACフレーム作成部
23
CRC計算部
24
セクション作成部
25
トランスポートパケット作成部
26
暗号化器
27
データ転送部
データ処理部16へ

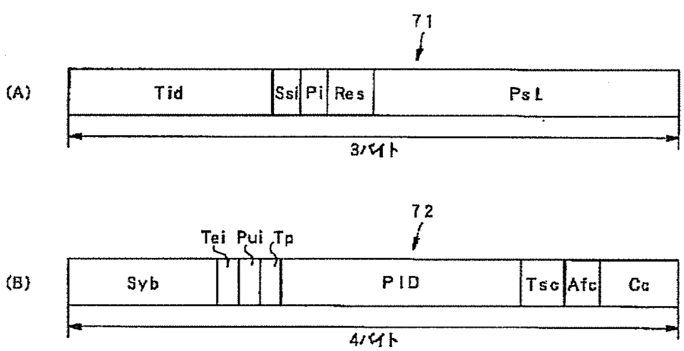
【図５】


0
4
8
16
31ビット
バージョン
IHL
TOS
Total Length
Identification
フラグ
Fragment Offset
TTL
Protocol
チェックサム
送信元IPアドレス
73
送信先IPアドレス
74
オプション

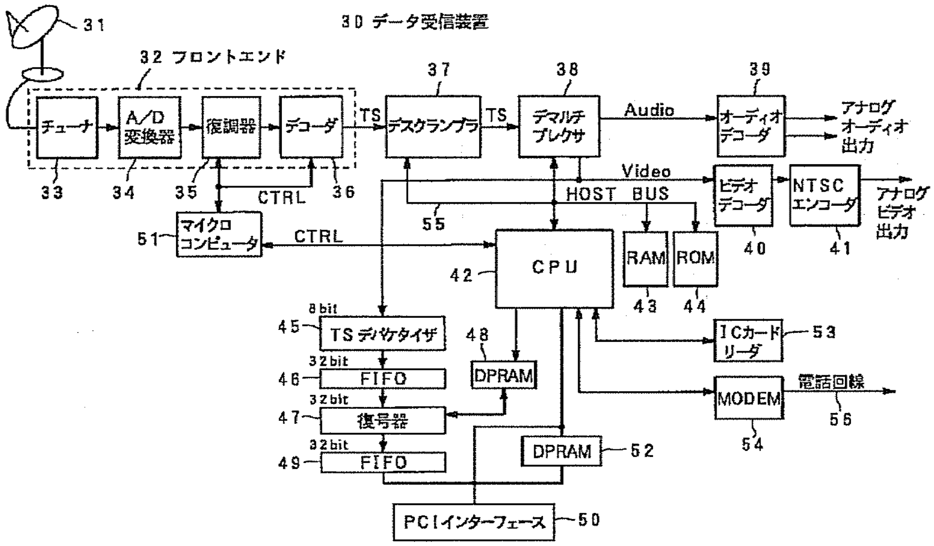
【図６】


70
3ビット PBL
1 CP
1 EN
1 PN
2 Rsv
16 Protocol Type
8ビット SSID
24ビット UDB1
UDB2
32 ビット(4バイト)
32ビット(4バイト)

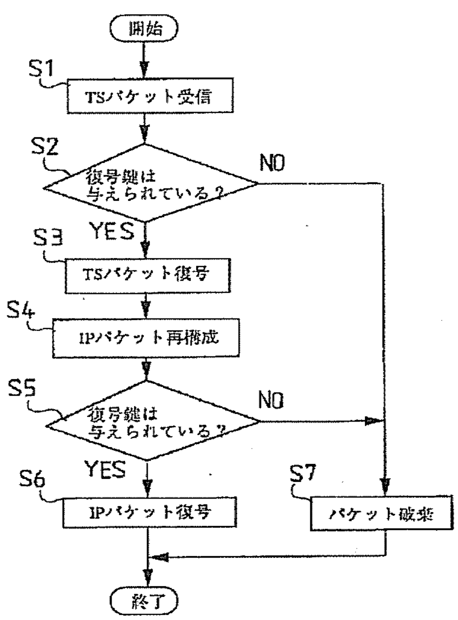
【図７】


(A)
71
Tid
Ssi
Pi
Res
PsL
3バイト
(B)
72
Tei
Pui
Tp
Syb
PID
Tsc
Afc
Cc
4バイト

【図８】



【図９】



【図１１】

80

	+0 / +2	+4 / +6	+8 / +aH / +cH / +eH
0H	識別子 1	マスクビット	識別子 1 の Session Key
10H	識別子 2	マスクビット	識別子 2 の Session Key
20H	識別子 3	マスクビット	識別子 3 の Session Key
30H	識別子 4	マスクビット	識別子 4 の Session Key
40H	識別子 5	マスクビット	識別子 5 の Session Key
50H	ENDコード		
	4バイト		8バイト

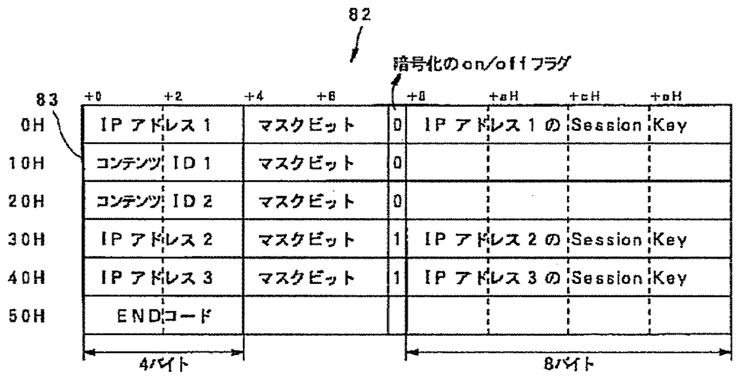
【図１２】

81

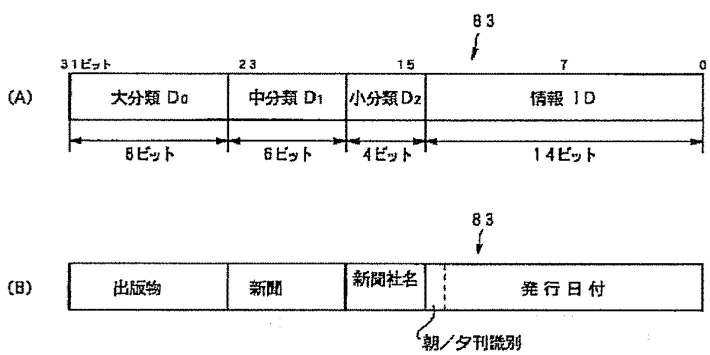
暗号化のon/offフラグ

	+0 / +2	+4 / +6		+8 / +aH / +cH / +eH
0H	IP アドレス 1	マスクビット	0	IP アドレス 1 の Session Key
10H	IP アドレス 2	マスクビット	1	IP アドレス 2 の Session Key
20H	IP アドレス 3	マスクビット	1	IP アドレス 3 の Session Key
30H	IP アドレス 4	マスクビット	1	IP アドレス 4 の Session Key
40H	IP アドレス 5	マスクビット	0	IP アドレス 5 の Session Key
50H	ENDコード			
	4バイト			8バイト

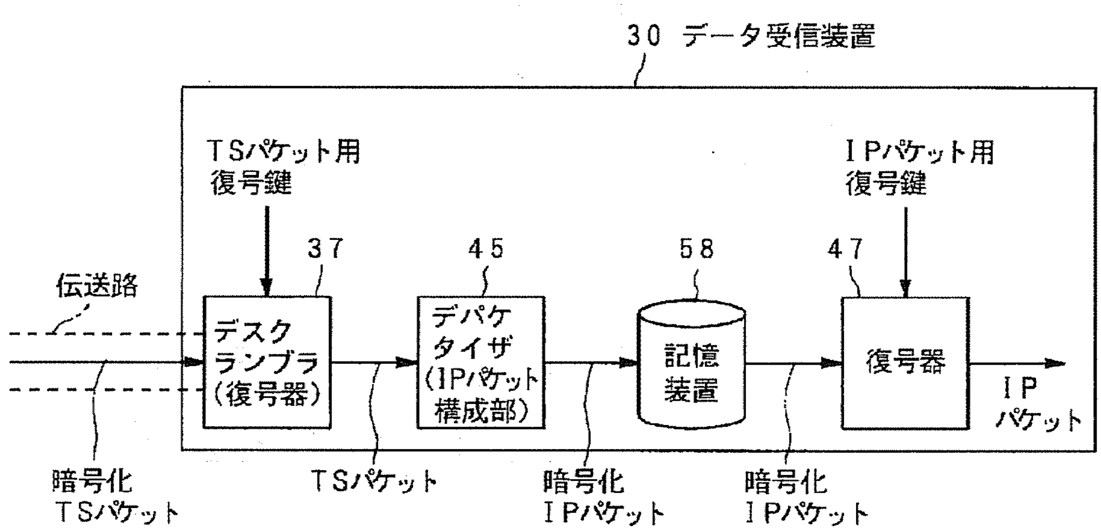
【図１３】


82
暗号化のon/offフラグ
83
+0
+2
+4
+6
+8
+aH
+cH
+eH
0H
10H
20H
30H
40H
50H
IP アドレス 1
コンテンツ ID 1
コンテンツ ID 2
IP アドレス 2
IP アドレス 3
ENDコード
マスクビット
0
1
IP アドレス 1 の Session Key
IP アドレス 2 の Session Key
IP アドレス 3 の Session Key
4バイト
8バイト

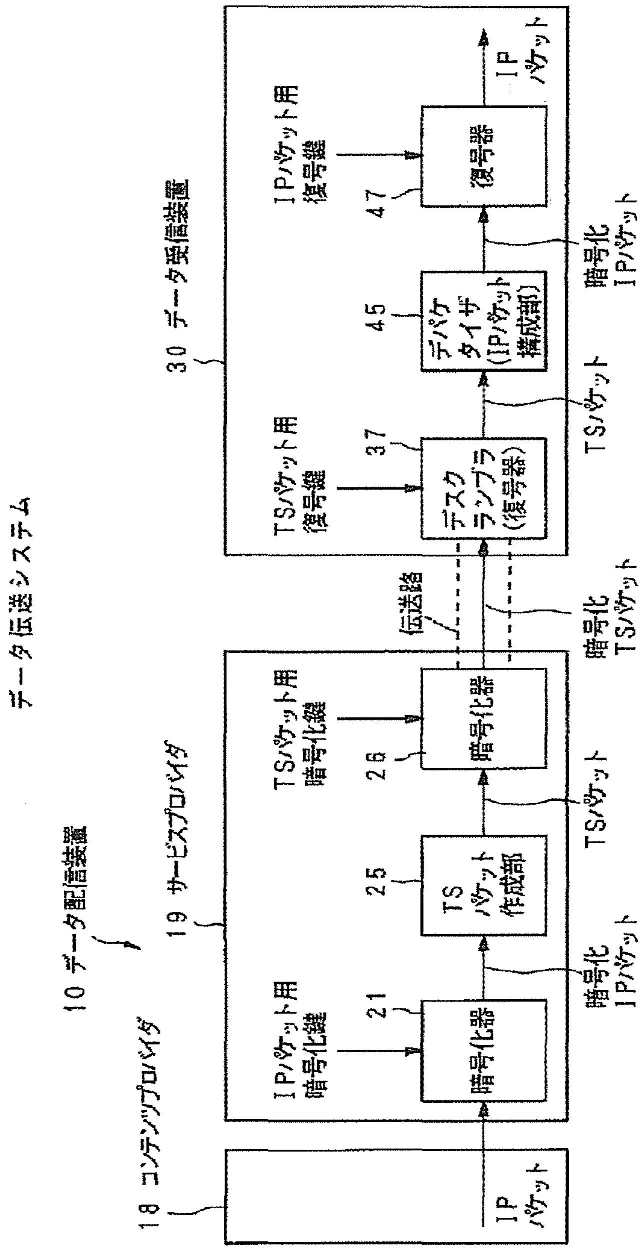
【図１４】


83
31ビット
23
15
7
0
(A)
大分類 D0
中分類 D1
小分類 D2
情報 ID
8ビット
6ビット
4ビット
14ビット
83
(B)
出版物
新聞
新聞社名
発行日付
朝／夕刊識別

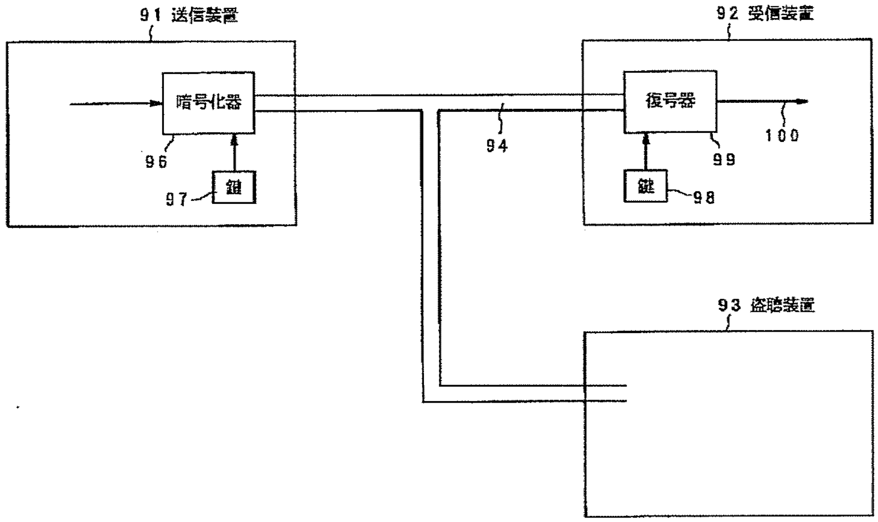
【図１６】


30 データ受信装置
TSパケット用
復号鍵
IPパケット用
復号鍵
37
45
58
47
伝送路
デスクランブラ
(復号器)
デパケタイザ
(IPパケット構成部)
記憶装置
復号器
IP
パケット
暗号化
TSパケット
TSパケット
暗号化
IPパケット
暗号化
IPパケット

【図１５】


データ伝送システム
10 データ配信装置
18 コンテンツプロバイダ
19 サービスプロバイダ
30 データ受信装置
IP パケット
IPパケット用暗号化鍵
21
暗号化器
暗号化 IPパケット
25
TS パケット作成部
TSパケット
TSパケット用暗号化鍵
26
暗号化器
伝送路
暗号化 TSパケット
TSパケット用復号鍵
37
デスクランブラ(復号器)
TSパケット
45
デパケタイザ(IPパケット構成部)
暗号化 IPパケット
IPパケット用復号鍵
47
復号器
IP パケット

【図１７】



Examples

Fig. 1 shows a protocol in a key distribution phase of a key distribution system equipped with an authentication function according to the present invention. A certificate issuing phase is the same as that of the conventional art.

(1) A terminal 1 generates distribution information C1 as follows, and sends the distribution information and its own certificate Cert1 to a terminal 2.

(a) A random number r1 is generated.

(b) $C1=g^{r1}$ modp

(2) The terminal 2 generates distribution information C2 as follows.

(a) A random number r2 is generated.

(b) $C2=g^{r2}$ modp

In addition, the terminal 2 generates R2 mentioned below as a response to the C1. Then, the terminal 2 sends the C2 and R2 together with its own certificate CERT2 to the terminal 1.

$R2=C1^{r2+x2}$ modp

(3) The terminal 1 calculates

h(Cert2)=y2::I D2

from the certificate Cert2 sent from the terminal 2 to acquire a public key y2 authenticated by a center for the terminal 2. Next, using the public key y2, the terminal 1 checks if

$R2=(C2\times y2)^{r1}$ modp

is satisfied. If it is satisfied, the terminal 1 authenticates that the communication counterpart is the terminal 2, and provides a common key for the terminal 2 by the following calculation. If it is not, this key distribution protocol is aborted.

$K12=C2^{r1}$ modp

Further, R1 mentioned below is generated from the second terminal as a response to a challenge C2. Then, the R1 is sent to the first terminal.

$R1=C2^{r1+x1}$ modp

(4) The terminal 2 calculates

h(Cert1)=y1::I D1

from the certificate Cert1 sent from the terminal 1 to acquire a public key y1 authenticated by the center for the terminal 1. Next, using the public key y1, the terminal 2 checks if

$R1=(C1\times y1)^{r2}$ modp

is satisfied. If it is satisfied, the terminal 2 authenticates that the communication counterpart is the terminal 1, and provides a common key for the terminal 1 by the following calculation. If it is not, this key distribution protocol is aborted.

$K21=C1^{r2modp}$

Note that $K12=K21=g^{r1\times r2}$ modp.

According to the above embodiment, to generate a response to a challenge from the counterpart, legitimate secret information is needed. Then, this response is verified using public information authenticated by the center. Therefore, this method can be said to be a key distribution system including direct counterpart authentication. The sharing of a key is achieved using the challenge received from the counterpart in a manner similar to the DH key distribution system. Further, the amount of calculation up to the sharing of a key is evaluated as follows. The evaluation of the amount of calculation is carried out based on the number of operations on modulo exponentiation. This is because, when the value of the modulo p in each calculation is set large (e.g., 512 bits) to ensure safety (to make it difficult to acquire secret information of terminals from public information), the operations on modulo exponentiation become a bottleneck of the entire calculation time. Both terminals need a total of four operations on modulo exponentiation as follows.

- once in the generation of a challenge
- once in the generation of a response
- once in the verification of the validity of the counterpart's response
- once in the generation of a shared key

Therefore, only one operation on modulo exponentiation is increased as compared to the key distribution system added with a conventional indirect authentication function. In the above embodiment, the authentication using a challenge and a response is configured with the key distribution. However, the authentication system may of course be handled independently.

Effect of the Invention

As is clear from the above explanations, a shared key can be changed every time without changing a certificate in the present invention. In addition, the counterpart is directly verified using the public key of the counterpart authenticated by the center, based on a response to a challenge generated by the terminal. In authenticating of the counterpart based on both a challenge and a response, secret information of the terminal is protected by including a secret random number in the response. The amount of calculation involved in the operation is four operations on modulo exponentiation, which is the minimum increase in the amount of calculation as compared to the conventional key distribution system that can only achieve indirect authentication.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **04-117826**

(43)Date of publication of application : **17.04.1992**

(51)Int.Cl. **H04L 9/28**

G09C 1/00

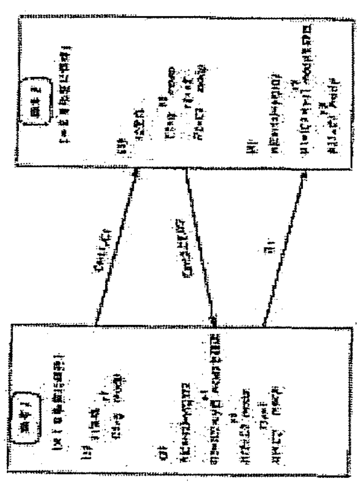
(21)Application number : **02-237498**

(22)Date of filing : **07.09.1990**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**

(72)Inventor : **MATSUZAKI NATSUME**
HARADA TOSHIHARU
TATEBAYASHI MAKOTO

(54) KEY-DELIVERY SYSTEM WITH VERIFICATION FUNCTION



(57)Abstract:

PURPOSE: To confirm an opposite party clearly by generating a response R2 through the use of its own secret information x2 and a random number r2 with respect to a challenge data C1 outputted from a 1st terminal equipment by a 2nd terminal equipment, allowing both the terminal equipments to verify each other and obtaining a common key.

CONSTITUTION: A terminal equipment 1 generates delivery information C1 and sends its own certificate Cert 1 to a terminal equipment 2. The terminal equipment 2 generates delivery information C2. Moreover, the terminal equipment 2 generates a response R2 with respect to the information C1, sends the information C2 and the response R2 together with its own certificate Cert 2 to the 1st terminal equipment 1. The terminal equipment

1 obtains a public key y2 of the terminal equipment 2 admitted by a center based on the certificate Cert 2 sent from the terminal equipment 2. Then the terminal equipment 1 verifies by using the public key y2 that the communication opposite party is the terminal equipment 2 and obtains the common key with the terminal equipment 2 according to the calculation shown in figure. The terminal equipment 2 obtains the public key y1 of the terminal equipment 1 admitted by the center based on the certificate Cert 1 sent from the terminal equipment 2. Then the terminal equipment 2 uses the public key y1 to verify it that the communication opposite party is the terminal equipment 1 and obtains the common key with the terminal equipment 1.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－117826

⑤Int. Cl.⁵　識別記号　庁内整理番号　㊸公開　平成4年(1992)4月17日
H 04 L 9/28
G 09 C 1/00　7922－5L
7117－5K　H 04 L 9/02　A
審査請求　未請求　請求項の数 1　（全7頁）

⑭発明の名称　認証機能付き鍵配送方式

㉑特　願　平2－237498
㉒出　願　平2(1990)9月7日

⑫発明者　松崎　なつめ　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑫発明者　原田　俊治　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑫発明者　館林　誠　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑪出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
⑭代理人　弁理士　小鍜治　明　外2名

明　細　書

1. 発明の名称

認証機能付き鍵配送方式

2. 特許請求の範囲

重複しない固有の識別情報を持った第1、第2の端末と、端末間を結ぶ通信路と、各端末が生成した公開情報に署名を施して証明書を発行するセンターとからなるシステムにおいて、証明書の発行時は、前記第1の端末は秘密情報x1を生成し、システムで公開の数pとpを法とする剰余環の原始元gを用いてx1をべきとし前記pを法とするgのべき乗剰余値y1を算出し、このy1を第1の公開情報としてセンターに通知し、前記第2の端末は秘密情報x2を生成し、x2をべきとし前記pを法とするgのべき乗剰余値y2を算出し、このy2を第2の公開情報としてセンターに通知し、センターは前記第1、2の公開情報に端末の識別情報を含めて、署名を施して証明書を生成し、各端末それぞれに配付し、鍵配送時、前記第1の端末は、前記通信路に接続し、前記センターから配付された第1の端末の証明書を格納して、通信路を通じて第2の端末に送信する第1の証明書格納手段と、乱数r1を生成する第1の乱数発生手段と、前記第1の乱数発生手段と前記通信路に接続し、前記r1をべきとし前記pを法とするgのべき乗剰余値C1を算出して、前記通信路を通じて第2の端末にデータC1を送信する第1の送信データ生成手段から構成され、前記第2の端末は、前記通信路に接続し、前記センターから送信された第2の端末の証明書を格納して、通信路を通じて第1の端末に送信する第2の証明書格納手段と、前記第1の端末から送信された第1の端末の証明書から第1の端末の第1の公開情報y1を求める第1の公開情報算出手段と、乱数r2を生成する第2の乱数発生手段と、前記第2の乱数発生手段と前記通信路に接続し、前記r2をべきとし前記pを法とするgのべき乗剰余値C2を算出して、前記通信路を通じて第1の端末にデータC2を送信する第2の送信データ生成手段と、前記第2の端末の秘密情報x2を格納する第1の秘密情報格納手段と、前記第1の秘密情報格納手段と前記第

２の乱数発生手段と前記通信路に接続し、前記乱数r2と第２の端末の秘密情報x2の和をべきとし、前記pを法とする前記送信データC1のべき乗剰余値R2を算出し、前記通信路を通じて第１の端末にデータR2を送信する第３の送信データ生成手段から構成され、前記第１の端末は、前記第２の端末から送信された第２の端末の証明書から第２の端末の公開情報y2を求める第２の公開情報算出手段と、前記第２の公開情報算出手段と前記第１の乱数発生手段と前記通信路に接続し、前記乱数r1をべきとし前記pを法とする前記C2とy2の積のべき乗剰余値を求め、これと前記第２の端末から送信された第３の送信データR2を比較してこれらが同じであることによって第２の端末を認証する第１の認証手段と、前記第１の端末の秘密情報x1を格納する第２の秘密情報格納手段と、前記第２の秘密情報格納手段と前記第１の乱数発生手段と前記通信路に接続し、前記乱数r1と第１の端末の秘密情報x1の和をべきとし、前記pを法とする前記第２の送信データC2のべき乗剰余値R1を算出し、前記通信路

を通じて第２の端末にデータR1を送信する第４の送信データ生成手段と、前記第１の乱数発生手段と前記通信路に接続し、乱数r1をべきとし前記pを法とする前記第２の端末から送信された第２の送信データC2のべき乗剰余値を、前記第２の端末との共有鍵とする第１の共有鍵生成手段から構成され、前記第２の端末は、前記第１の公開情報算出手段と前記第２の乱数発生手段と前記通信路に接続し、前記乱数r2をべきとし前記pを法とする前記C1とy1の積のべき乗剰余値を求め、これと前記第１の端末から送信された第４の送信データR1を比較してこれらが同じであることによって第１の端末を認証する第２の認証手段と、前記第２の乱数発生手段と前記通信路に接続し、乱数r2をべきとし前記pを法とする前記第１の端末から送信された第１の送信データC1のべき乗剰余値を前記第１の端末との共有鍵とする第２の共有鍵生成手段から構成される認証機能付き鍵配送方式。

3. 発明の詳細な説明

産業上の利用分野

本発明は、互いにチャレンジとレスポンスをやり取りすることによって相手を認証し、その結果秘密の共有鍵を得る認証機能付き鍵配送方式に関する。なお、相手からのレスポンスの正当性確認に用いる相手端末の公開情報は、信頼のおけるセンターがあらかじめ生成した証明書によって保証されている。

従来の技術

暗号系に秘密鍵暗号方式を用いる場合、各通信対で対ごとに異なった鍵を秘密に共有する必要がある。従来の集中鍵配送方式では、鍵共有のたびに、ネットワーク上にある鍵配送センターが各共有鍵を生成し、端末に秘密に配送する必要があるため、鍵配送センターに鍵負担が集中し、端末数の多い大規模ネットワークには適していない。一方、鍵の配送と同時に、鍵を共有する相手をきちんと認証することも要望されている。したがって、ここでは認証機能を組み込んだ分散型の鍵配送方

式について説明する。分散型の鍵配送方法として、1976年にディフィとヘルマン(Diffe、Hellman)によって提案されたディエイチ（ＤＨ）鍵配送方式がある。詳細については、アイイーイーイー・トランザクションズ・オン・インフォメーション・セオリー(IEEE Trans. Inf. Theory IT-22, 6, pp644～654(Nov. 1976))を参照すること、ＤＨ鍵配送方式は、有限体GF(p)上での離散対数問題が難しいことに安全性の根拠をおいている。ここではこれに認証機能を組み込んだ方法について説明する。認証を可能とするため、信頼のおけるセンター発行の証明書を用いる。

ＤＨ鍵配送方式（第１の従来例）

以下、この第１の従来例の手順を、センターによる証明書の発行のフェーズと、端末１と端末２の間の鍵配送のフェーズに分けて説明する。

<証明書の発行フェーズ>

（Ｉ）システムの構築時、素数pとGF(p)の原始元gを決定し各端末に公開する。ここで安全性を確保するため、pは例えば512ビット程度の大きな素

数に決定する。

（２）端末１は秘密情報x1を生成して、$y1=g^{x1}$ modpを計算する。

なお、ここで'X modp'は値Xをpで除した時の剰余を示す。

（３）端末１はy1と名前、住所など自分を特定できる情報（識別情報、又はＩＤ情報と称する）ＩＤ１を信頼のおけるセンターに送信し、証明書を請求する。

（４）センターは端末１の正当性を調べ、センターだけが知っている秘密変換fを用いて、証明書Cert1を生成し、例えば磁気カード等に格納して端末１に配付する。

$Cer1=f(y1 \| ID1)$

ここで、‖は連結を示している。なお、秘密変換fの逆変換hはシステムにおいて公開であるとする。従って、Cert1を得た任意の端末はh(Cert1)を計算することで、センターによって保証された端末１の公開情報y1を得ることができる。端末２についても同様に証明書Cert2を発行する。

＜鍵配送フェーズ＞

（１）端末１は自身の証明書Cert1を端末２に、端末２は自身の証明書Cert2を端末１にそれぞれ配送する。

（２）端末１は$h(Cert2)=y2 \| ID2$を計算し、自分の秘密情報x1を用いて、

$K12=y2^{x1} \mathrm{modp}=g^{x1 \times x2} \mathrm{modp}$

を求める。

（３）一方、端末２は$h(Cert1)=y1 \| ID1$を計算し、自分の秘密情報x2を用いて、

$K21=y1^{x2} \mathrm{modp}=g^{x1 \times x2} \mathrm{modp}$

を求める。なお、K12=K21は端末１と２の間の共有鍵である。

ところで、暗号通信で用いられる暗号鍵は、安全上時々変更することが望ましい。上記で述べたＤＨ鍵配送方式では共有鍵を変更するのにもう１度センターに依頼して証明書を発行してもらう必要があり、非常に手間である。

第２の従来例

特開昭61-30829では、証明書は変更せずに共有

鍵を変更する方法が提案されている。証明書の発行フェーズは第１の従来例と同じである。第２図に鍵配送フェーズの手順を示している。端末１、２間の動作を以下に示す。

（１）端末１は次のようにして配送情報Z12を生成し、これと自分の証明書Cert1を端末２に送付する。

(a)乱数r1を発生する。

(b)$Z12=y1^{r1}$ modp　　　・・・(1)

（２）端末２は次のようにして配送情報Z21を生成し、これと自分の証明書Cert2を端末１に送付する。

(a)乱数r2を発生する。

(b)$Z21=y2^{r2}$ modp　　　・・・(2)

また、端末１から送付されてきた情報を用いて、以下のとおり端末１との共有鍵K21を生成する。

(a)Cert1より、$h(Cert1)=y1 \| ID1$を計算し、センターの認めた端末１の公開情報y1を得る。

(b)端末１からの配送情報Z12より次のように共有鍵を算出する。

$K21=(Z12 \times y1^{r2})^{x2}$ modp　・・・(3)

（３）端末１は、端末２から送付されてきた情報を用いて、以下のとおり端末２との共有鍵共有鍵K12を生成する。

(a)Cert2より、$h(Cert2)=y2 \| ID2$を計算し、センターの認めた端末２の公開情報y2を得る。

(b)端末２からの配送情報Z21より次のように共有鍵を算出する。

$K12=(Z21 \times y2^{r1})^{x1}$ modp　・・・(4)

なお、端末１における共有鍵K12と端末２における共有鍵生成手段K21は(1)～(4)式より同じ値になる。

$K12=(Z21 \times y2^{r1})^{x1} \mathrm{modp}=(y2^{r2+r1})^{x1} \mathrm{modp}=g^{x1 \times x2 \times (r1+r2)} \mathrm{modp}$

$K21=(Z12 \times y1^{r2})^{x2} \mathrm{modp}=(y1^{r2+r1})^{x2} \mathrm{modp}=g^{x1 \times x2 \times (r1+r2)} \mathrm{modp}$

発明が解決しようとする課題

第１の従来例では、特定の２者間の鍵が毎回同じであるという欠点がある。第１の従来例で毎回の鍵を変更するためには、センターにおいて端末

の証明書を作り替えてもらわなくてはならず、かなり手間がかかる。また、第2の従来例では証明書を変更せずに毎回の鍵を変更することができる。但し、この方式における認証機能は間接的な認証であり、自分の認識している相手とのみ同じ鍵を共有できることが保証されているというものであった。従って、きちんと相手からのデータにより相手を認証するものではない。さらに共有鍵を得るには、配送データの生成に1回、共有鍵の生成に2回の計3回のべき乗剰余演算が必要である。

本発明の認証機能付き鍵配送方式は、上述の問題点に鑑みて試みられたもので、証明書を変更せずに毎回の鍵を変更する鍵配送方式であって、さらに、相手にデータ（チャレンジ）を与え、その応答（レスポンス）によってきちんと相手を確認する認証機能を付加した鍵配送方式を提供することを目的とする。なお、この際に従来の間接的認証を付加した方法に比べて計算量の増加を最小限とする。

-11-

課題を解決するための手段

前記目的を達成するために、本発明における認証機能付き鍵配送方式は、重複しない固有の識別情報を持った第1、第2の端末と、端末間を結ぶ通信路と、各端末が生成した公開情報に署名を施して証明書を発行する信頼のおけるセンターからなるシステムにおいて、証明書の発行時は、前記第1の端末は秘密情報x1を生成し、システムで公開の数pとpを法とする剰余環の原始元gを用いてx1をべきとし前記pを法とするgのべき乗剰余値y1を算出し、このy1を第1の公開情報としてセンターに通知し、前記第2の端末は秘密情報x2を生成し、x2をべきとし前記pを法とするgのべき乗剰余値y2を算出し、このy2を第2の公開情報としてセンターに通知し、センターは前記第1、2の公開情報に端末の識別情報を含めて、署名を施して証明書を生成し、各端末それぞれに配付し、鍵配送時、前記第1の端末は、前記通信路に接続し、前記センターから配付された第1の端末の証明書を格納して、通信路を通じて第2の端末に送信する第1

-12-

の証明書格納手段と、乱数r1を生成する第1の乱数発生手段と、前記第1の乱数発生手段と前記通信路に接続し、前記r1をべきとし前記pを法とするgのべき乗剰余値C1を算出して、前記通信路を通じて第2の端末にデータC1を送信する第1の送信データ生成手段から構成され、前記第2の端末は、前記通信路に接続し、前記センターから送信された第2の端末の証明書を格納して、通信路を通じて第1の端末に送信する第2の証明書格納手段と、前記第1の端末から送信された第1の端末の証明書から第1の端末の第1の公開情報y1を求める第1の公開情報算出手段と、乱数r2を生成する第2の乱数発生手段と、前記第2の乱数発生手段と前記通信路に接続し、前記r2をべきとし前記pを法とするgのべき乗剰余値C2を算出して、前記通信路を通じて第1の端末にデータC2を送信する第2の送信データ生成手段と、前記第2の端末の秘密情報x2を格納する第1の秘密情報格納手段と前記第1の秘密情報格納手段と前記第2の乱数発生手段と前記通信路に接続し、前記乱数r2と第2の端末の

-13-

秘密情報x2の和をべきとし、前記pを法とする前記送信データC1のべき乗剰余値R2を算出し、前記通信路を通じて第1の端末にデータR2を送信する第3の送信データ生成手段から構成され、前記第1の端末は、前記第2の端末から送信された第2の端末の証明書から第2の端末の公開情報y2を求める第2の公開情報算出手段と、前記第2の公開情報算出手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数r1をべきとし前記pを法とする前記C2とy2の積のべき乗剰余値を求め、これと前記第2の端末から送信された第3の送信データR2を比較してこれらが同じであることによって第2の端末を認証する第1の認証手段と、前記第1の端末の秘密情報x1を格納する第2の秘密情報格納手段と、前記第2の秘密情報格納手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数r1と第1の端末の秘密情報x1の和をべきとし、前記pを法とする前記第2の送信データC2のべき乗剰余値R1を算出し、前記通信路を通じて第2の端末にデータR1を送信する第4の送信データ生成手

-14-

段と、前記第1の乱数発生手段と前記通信路に接続し、乱数r1をべきとし前記pを法とする前記第2の端末から送信された第2の送信データC2のべき乗剰余値を、前記第2の端末との共有鍵とする第1の共有鍵生成手段から構成され、前記第2の端末は、前記第1の公開情報算出手段と前記第2の乱数発生手段と前記通信路に接続し、前記乱数r2をべきとし前記pを法とする前記C1とy1の積のべき乗剰余値を求め、これと前記第1の端末から送信された第4の送信データR1を比較してこれらが同じであることによって第1の端末を認証する第2の認証手段と、前記第2の乱数発生手段と前記通信路に接続し、乱数r2をべきとし前記pを法とする前記第1の端末から送信された第1の送信データC1のべき乗剰余値を前記第1の端末との共有鍵とする第2の共有鍵生成手段から構成される。

作用

第2の端末は第1の端末の出力するチャレンジデータC1に対するレスポンスR2を、自分の秘密情報x2と自分の生成した乱数r2を用いて生成する。

従って、このレスポンスは正規の第2の端末しか生成することができない。第1の端末はこのレスポンスを、第2の端末の証明書から得た正規の公開情報y2によって認証する。また、レスポンスに自分の生成した秘密の乱数r2を含めているため、第1の端末および第3者はレスポンスから第2の端末の秘密情報x2を得ることはできない。同様に端末2はチャレンジデータC2に対するレスポンスR1により端末1を認証する。そして互いに相手を認証した後、相手からのチャレンジデータを用いて共有鍵を求める。

実施例

第1図は、本発明の認証機能付き鍵配送方式の鍵配送フェーズにおけるプロトコルを示す。証明書発行フェーズは従来例と同じである。

（1）端末1は次のようにして配送情報C1を生成し、これと自分の証明書Cert1を端末2に送付する。

(a)乱数r1を発生する。

(b)$C1=g^{r1}$ modp

（2）端末2は次のようにして配送情報C2を生成する。

(a)乱数r2を発生する。

(b)$C2=g^{r2}$ modp

また、前記C1に対するレスポンスとして以下のR2を生成する。そして自分の証明書CERT2とともに前記C2, R2を第1の端末に送信する。

$R2=C1^{r2+x2}$ modp

（3）端末1は端末2から送信された証明書Cert2から

h(Cert2)=y2‖ID2

を計算し、センターが認めた端末2の公開鍵y2を得る。次に、この公開鍵y2を用いて、

$R2=(C2\times y2)^{r1}$ modp

が成り立つことを確かめる。もし成り立てば、通信相手が端末2であることを認証し、次の計算で端末2との共有鍵を求める。異なっていれば、この鍵配送プロトコルを取りやめる。

$K12=C2^{r1}$ modp

また、前記第2の端末からチャレンジC2に対す

るレスポンスとして以下のR1を生成する。そして第1の端末に送信する。

$R1=C2^{r1+x1}$ modp

（4）端末2は端末1から送信された証明書Cert1から

h(Cert1)=y1‖ID1

を計算し、センターが認めた端末1の公開鍵y1を得る。次に、この公開鍵y1を用いて、

$R1=(C1\times y1)^{r2}$ modp

が成り立つことを確かめる。もし成り立てば、通信相手が端末1であることを認証し、次の計算で端末1との共有鍵を求める。異なっていれば、この鍵配送プロトコルを取りやめる。

$K21=C1^{r2}$ modp

なお、$K12=K21=g^{r1\times r2}$ modpである。

この実施例において、相手からチャレンジに対するレスポンスを生成するためには、正規の秘密情報が必要である。そして、このレスポンスをセンターの認めた公開情報を用いて確認する。このため、この方法は直接的な相手認証を含んだ鍵配

送方式であるといえる。なお、鍵の共有は相手からうけたチャレンジを用いDH鍵配送方式と同様にして行なう。また、鍵共有までの計算量については以下の通り評価する。なお、計算量の評価は、べき乗剰余演算の回数を行なう。これは、安全性を確保する（公開情報から端末の秘密情報を得ることを困難にする）ために各計算の法pの数を大きく（例えば512ビット）取ると、べき乗剰余演算が全体の計算時間のネックとなるためである。双方の端末ともに、

・チャレンジの生成に1回
・レスポンスの生成に1回
・相手のレスポンスの正当性確認に1回
・共有鍵の生成に1回

の計4回のべき乗剰余演算が必要である。従って、従来の間接的な認証機能が付加された鍵配送方式に比べてわずか1回のべき乗剰余演算が増加しているだけである。なお、この実施例では、チャレンジとレスポンスを用いた認証を鍵配送と合わせて構成したが、認証方式単独として取り扱ってもよいことは言うまでもない。

発明の効果

以上の説明から明らかなように本発明は、証明書を変更せずに毎回の共有鍵を変更することができる。また、相手を自身が発したチャレンジに対する応答を、センターの認めた相手の公開鍵を用いて直接的に確認する。チャレンジとレスポンスによる相手認証では、レスポンスに秘密の乱数を含めることによって端末の秘密情報を保護している。また、これにかかる計算量はべき乗剰余演算4回であり、間接的な認証しかできなかった従来の鍵配送方式と比べても最小限の計算量の増加となっている。

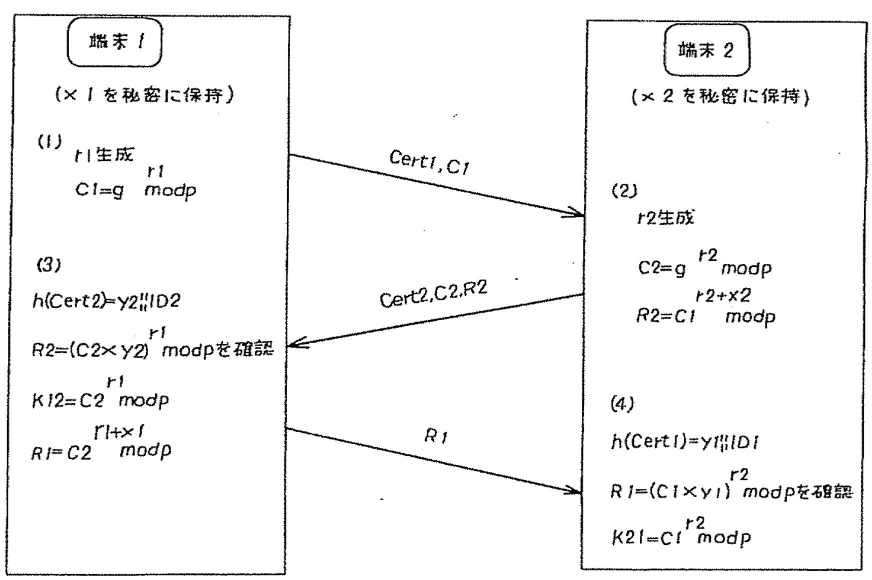
4．図面の簡単な説明

第1図は本発明の認証機能付き鍵配送方式における一実施例の鍵配送フェーズプロトコル図、第2図は従来における鍵配送フェーズプロトコル図である。

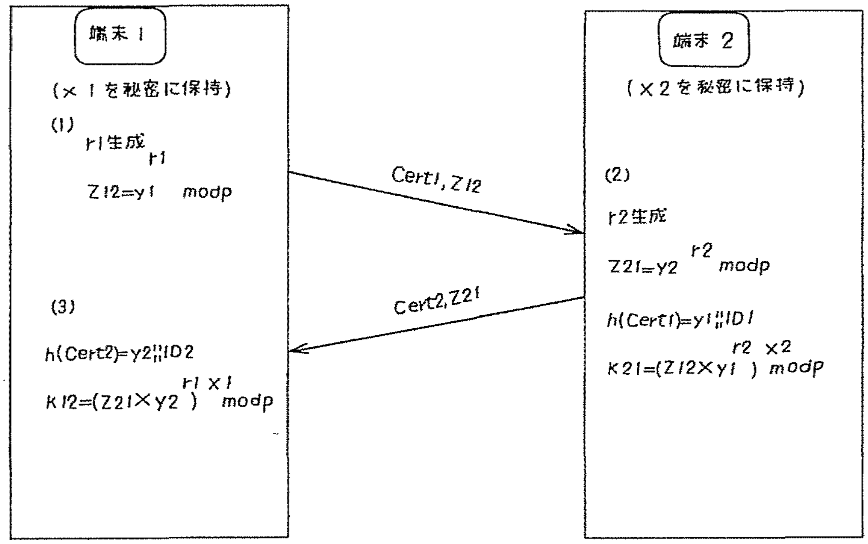
代理人の氏名　弁理士　小鍜治　明　ほか2名

-19-　-20-

第1図



第 2 図


端末 1
(x 1 を秘密に保持)
(1)
r1生成
Z12=y1 r1 modp
(3)
h(Cert2)=y2||ID2
K12=(Z21×y2) r1 x1 modp
Cert1, Z12
Cert2,Z21
端末 2
(x 2 を秘密に保持)
(2)
r2生成
Z21=y2 r2 modp
h(Cert1)=y1||ID1
K21=(Z12×y1) r2 x2 modp

OTHER PUBLICATIONS

Chun, B.N., et al., "Virtual Network Transport Protocols for Myrinet," IEEE Micro, Jan./Feb. 1998 at 53–63.
Cisco Systems Inc., "LocalDirector Hot–Standby Faiilover: Product Overview," www.cisco.com/univercd/cc/td/doc/product/iaabu/localdir/ld20rns/ldicgd/ld3_ch5.htm, 1998.
Damani, O., et al., "ONE–IP: techniques for hosting a service on a cluster of machines," Computer Networks and ISDN Systems, vol. 29, 1997 at 1019–1027.
Fox, A., et al., "Cluster–Based Scalable Network Services," 16th ACM Symposium on Operating systems Principles, Oct. 5–8, 1997 at 78–91.
Ghormley, D.P., et al., "GLUnix: A Global Layer Unix for a Network of Workstations," Software–Practice and Experience, vol. 28, No. 9, Jul. 25, 1998 at 929–961.
Huang, Y., et al., "Software Implemented Fault Tolerance: Technologies and Experience," 23rd International Symposium on Fault–Tolerant Computing, Jun. 22–24, 1993 at 2–9.
Hunt, G.D.H., et al., "Network Dispatcher: a connection router for scalable Internet services," Computer Networks and ISDN Systems, vol. 30, 1998 at 347–357.
Hwang, K., et al., *Scalable Parallel Computing*, WCB McGraw–Hill, 1998 at 366–377, 453–564.
Kurcewicz, M., et al., "A Distributed WWW Cache," Computer Networks and ISDN Systems, vol. 30, 1998 at 2261–2267.
Mendiratta, V.B., "Reliability Analysis of Clustered Computing Systems," 9th International Symposium on Software Reliability Engineering, Nov. 4–7, 1998 at 268–272.
Parker, T., "QualixHA+," Unix Review, Mar. 1998 at 59–61.
Short, R., et al., "Windows NT Clusters for Availability and Scalabilty," Proceedings, IEEE COMPCON '97, Feb. 23–26, 1997 at 8–13.
Taschek, J., "ZD Internet Lab; A Well–Balanced Web," www.zdnet.com/icom/zdlabs/load.balance/, Feb. 23, 1998.
Thaler, D.G., et al., "Using Name–Based Mappings to Increase Hit Rates," IEEE/ACM Transactions on Networking, vol. 6, No. 1, Feb. 1998 at 1–14.
Valence Research, Inc., "Convoy Cluster Software; Product Overview," www.valence.com/convoy/main.html.
Venkataraman, S., et al., "Memory Management for Scalable Web Data Servers," 13th International Conference on Data Engineering, Apr. 7–11, 1997 at 510–519.

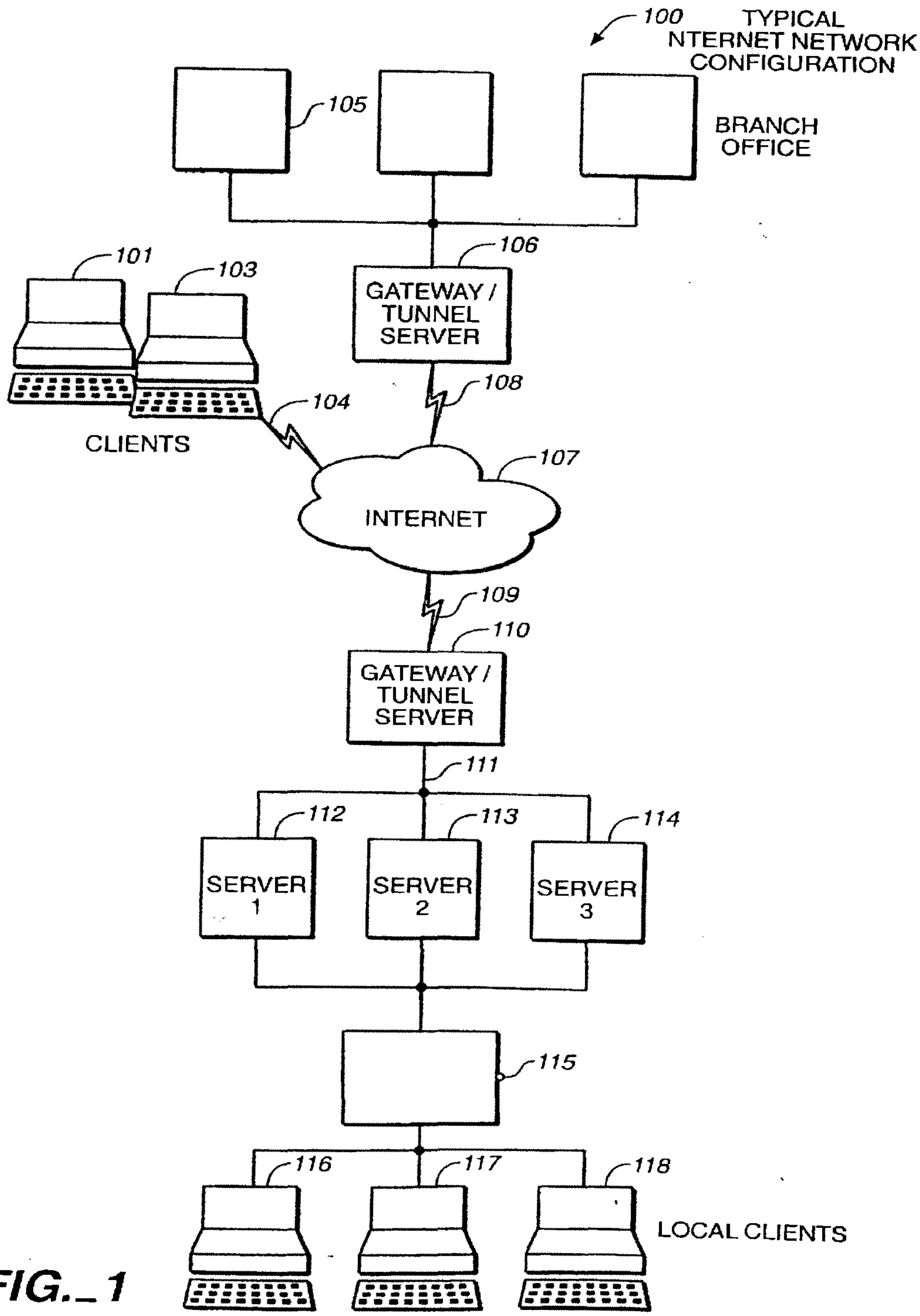

100 TYPICAL
NTERNET NETWORK
CONFIGURATION
105
BRANCH
OFFICE
101
103
106
GATEWAY /
TUNNEL
SERVER
108
104
CLIENTS
107
INTERNET
109
110
GATEWAY /
TUNNEL
SERVER
111
112
113
114
SERVER
1
SERVER
2
SERVER
3
115
116
117
118
LOCAL CLIENTS

FIG._1

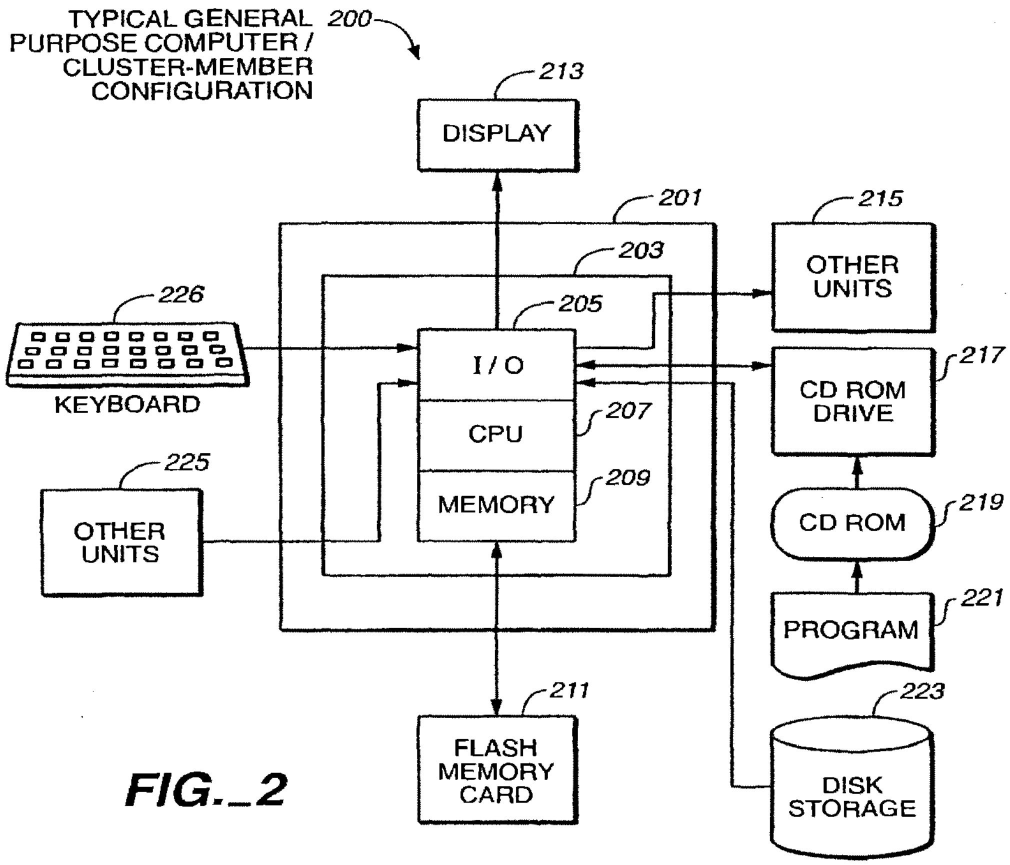

TYPICAL GENERAL PURPOSE COMPUTER / CLUSTER-MEMBER CONFIGURATION
200
213
DISPLAY
201
215
203
OTHER UNITS
226
205
I / O
217
CD ROM DRIVE
KEYBOARD
CPU
207
225
209
MEMORY
CD ROM
219
OTHER UNITS
221
PROGRAM
211
223
FLASH MEMORY CARD
DISK STORAGE

FIG._2

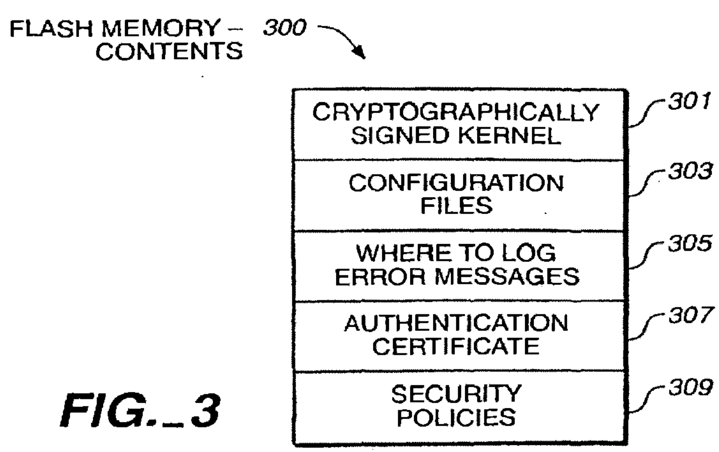
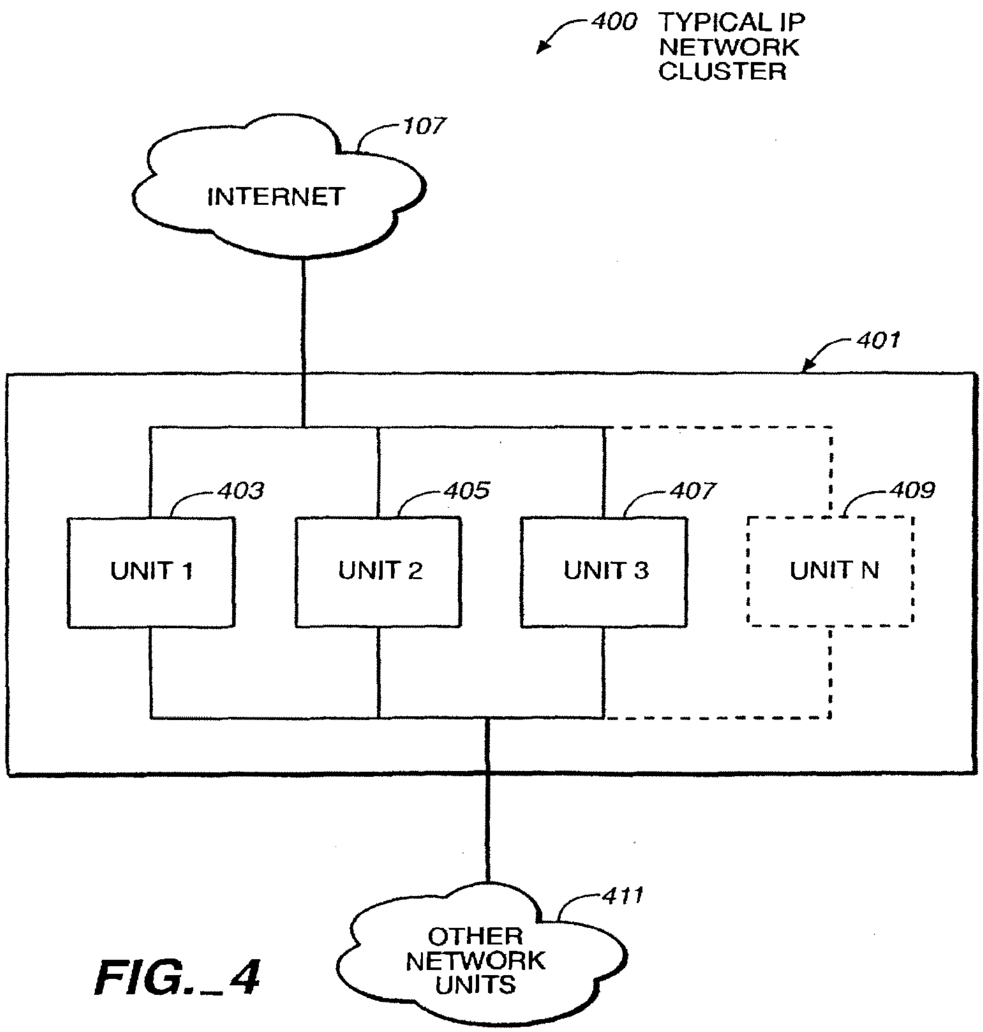

FLASH MEMORY – CONTENTS
300
CRYPTOGRAPHICALLY SIGNED KERNEL
301
CONFIGURATION FILES
303
WHERE TO LOG ERROR MESSAGES
305
AUTHENTICATION CERTIFICATE
307
SECURITY POLICIES
309

FIG._3



400 TYPICAL IP NETWORK CLUSTER
107
INTERNET
401
403
405
407
409
UNIT 1
UNIT 2
UNIT 3
UNIT N
411
OTHER NETWORK UNITS

FIG._4

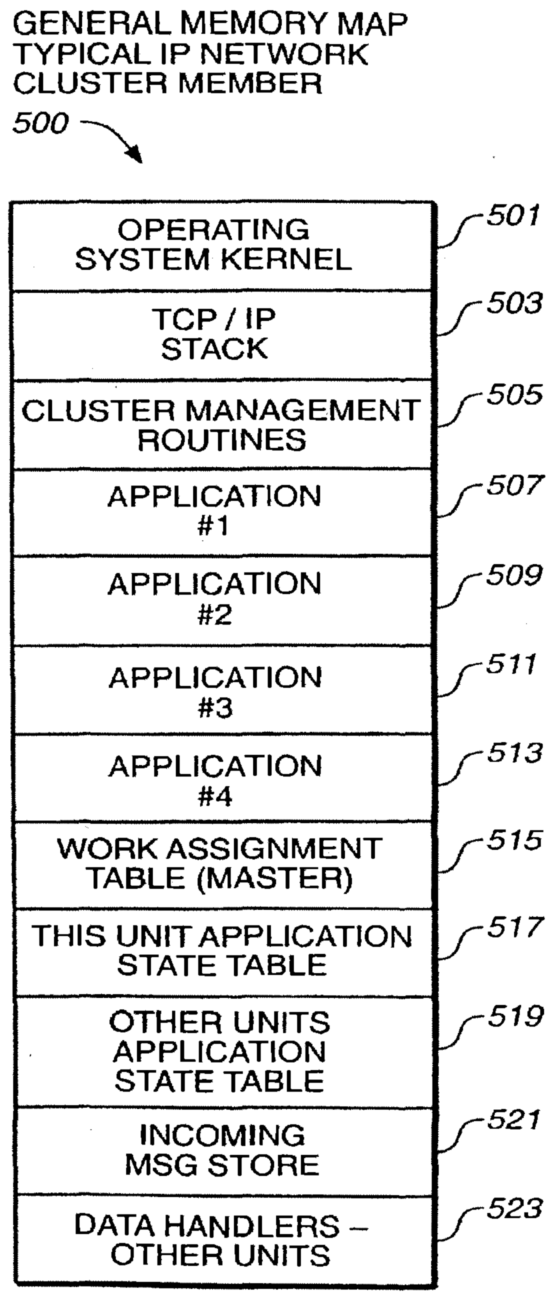
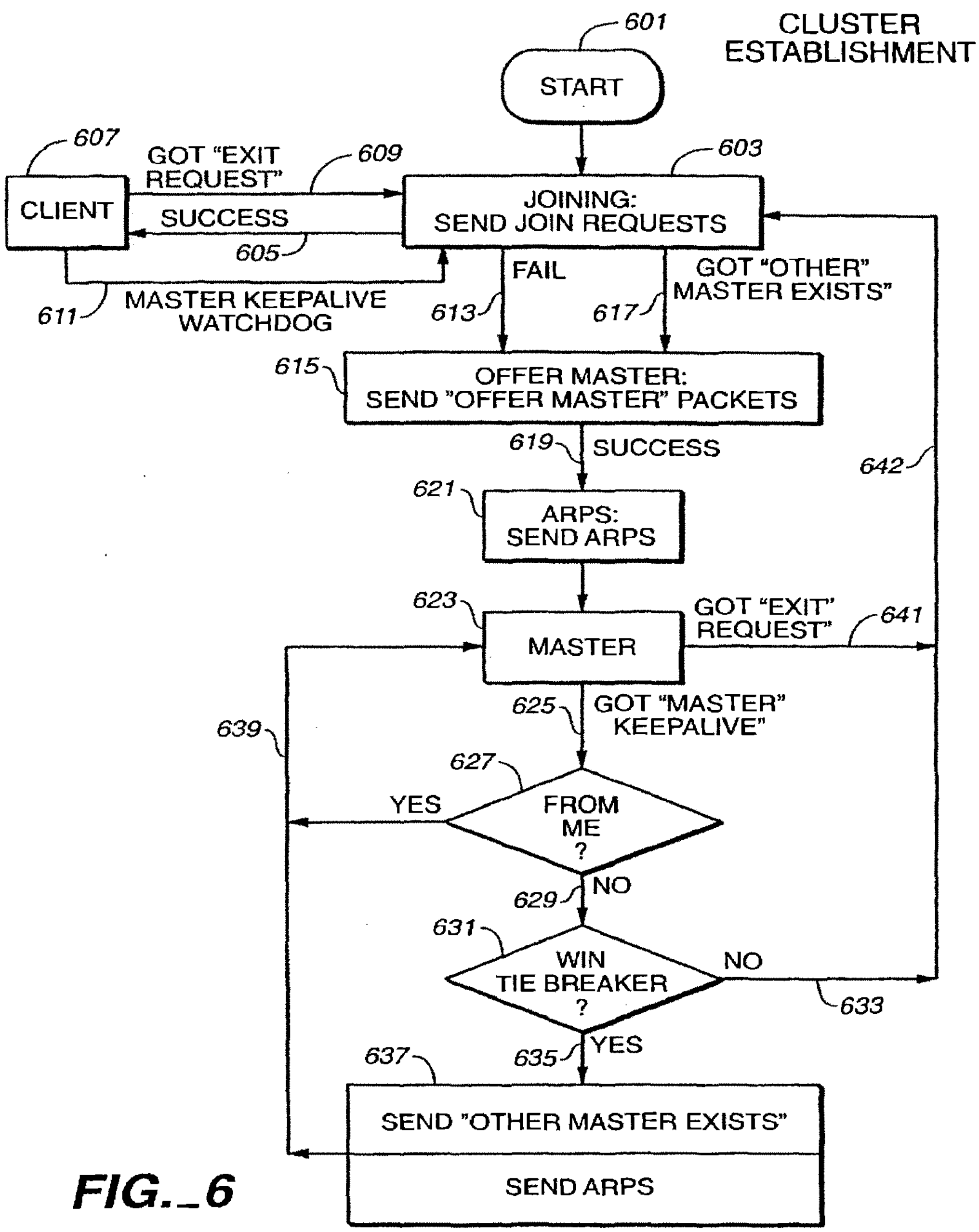

GENERAL MEMORY MAP
TYPICAL IP NETWORK
CLUSTER MEMBER
500
OPERATING
SYSTEM KERNEL
501
TCP / IP
STACK
503
CLUSTER MANAGEMENT
ROUTINES
505
APPLICATION
#1
507
APPLICATION
#2
509
APPLICATION
#3
511
APPLICATION
#4
513
WORK ASSIGNMENT
TABLE (MASTER)
515
THIS UNIT APPLICATION
STATE TABLE
517
OTHER UNITS
APPLICATION
STATE TABLE
519
INCOMING
MSG STORE
521
DATA HANDLERS –
OTHER UNITS
523

FIG._5



601
CLUSTER ESTABLISHMENT
START
607
CLIENT
GOT "EXIT REQUEST"
609
SUCCESS
605
603
JOINING: SEND JOIN REQUESTS
611
MASTER KEEPALIVE WATCHDOG
FAIL
613
GOT "OTHER" MASTER EXISTS"
617
615
OFFER MASTER: SEND "OFFER MASTER" PACKETS
619
SUCCESS
642
621
ARPS: SEND ARPS
623
MASTER
GOT "EXIT" REQUEST"
641
639
625
GOT "MASTER" KEEPALIVE"
627
YES
FROM ME ?
NO
629
631
WIN TIE BREAKER ?
NO
633
637
635
YES
SEND "OTHER MASTER EXISTS"
SEND ARPS

FIG._6

FIG._7

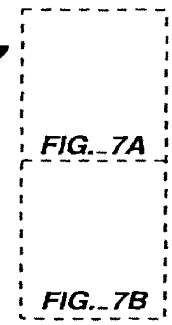


FIG._7A

TCP FAILOVER STATE 700

Initial State (Only need to send once) 702

Source IP Address + Port
Destination IP Address + Port
Maximum Segment Size
MSS + Options Size

Essential State (Send on each state change) 701

Flags: No Delay, No Options, Request Window Scaling, Receive Window Scaling, Request Timestamp, Receive Timestamp, Permit Selective ACK
Send "Next" Sequence Number
Window Update Segment Sequence Number
Window Update Segment Acknowledgement Number
Send Window
Receive "Next" Sequence Number
Receive "Advertized" Window
Send Window Scaling
Receive Window Scaling
Recent Timestamp Echo Data

703

Calculable State (Don't Send)

State = ESTABLISHED
Retransmit Time = None
Probe Time = Now
TCP Keepalive Time = Now
2MSL Time = None
Retransmit Time Shift = 0
Current Retransmit = Initial Value
Consecutive Duplicate Acks Received = 0
Force Output = 0;
Send "Unacknowledged" Sequence Number = Send "Next" Sequence Number
Send "Urgent Pointer" = Send "Unacknowledged" Sequence Number
Highest Sequence Number Sent = Send "Next" Sequence Number
Send Initial Segment Sequence Number = 0
Receive Window = Amount of space left in socket receive buffer
Receive "Urgent Pointer" = Receive "Next" Sequence Number
Receive Initial Segment Sequence Number = 0
Congestion Control Window = Initial Value
Congestion Control Window Linear/Exponential Threshold = Initial Value
Inactivity Time = 0
Estimated Round Trip Time = 0
Sequence Number Being Timed = 0
Smoothed Round Trip Time = Initial Value
Variance In Round Trip Time = Initial Value
Minimum Round Trip Time Allowed = Initial Value
Largest Window Offered by Peer = 0
Out Of Band Data = None
Send Pending Window Scaling = Send Window Scaling
Receive Pending Window Scaling = Receive Window Scaling
Timestamp Echo Data Update Time = 0
Last Ack Sent Sequence Number = Receive "Next" Sequence Number
Send Connection Count = 0
Receive Connection Count = 0;
Connection Duration = 0;
Number of Round Trip Time Samples = 0;
Number of TCP Keepalive Probes = Initial Value
Interval Between TCP Keepalive Probes = Initial Value
Time Before First TCP Keepalive Probe = Initial Value
Maximum Idle Time = Initial Value

FIG._7B

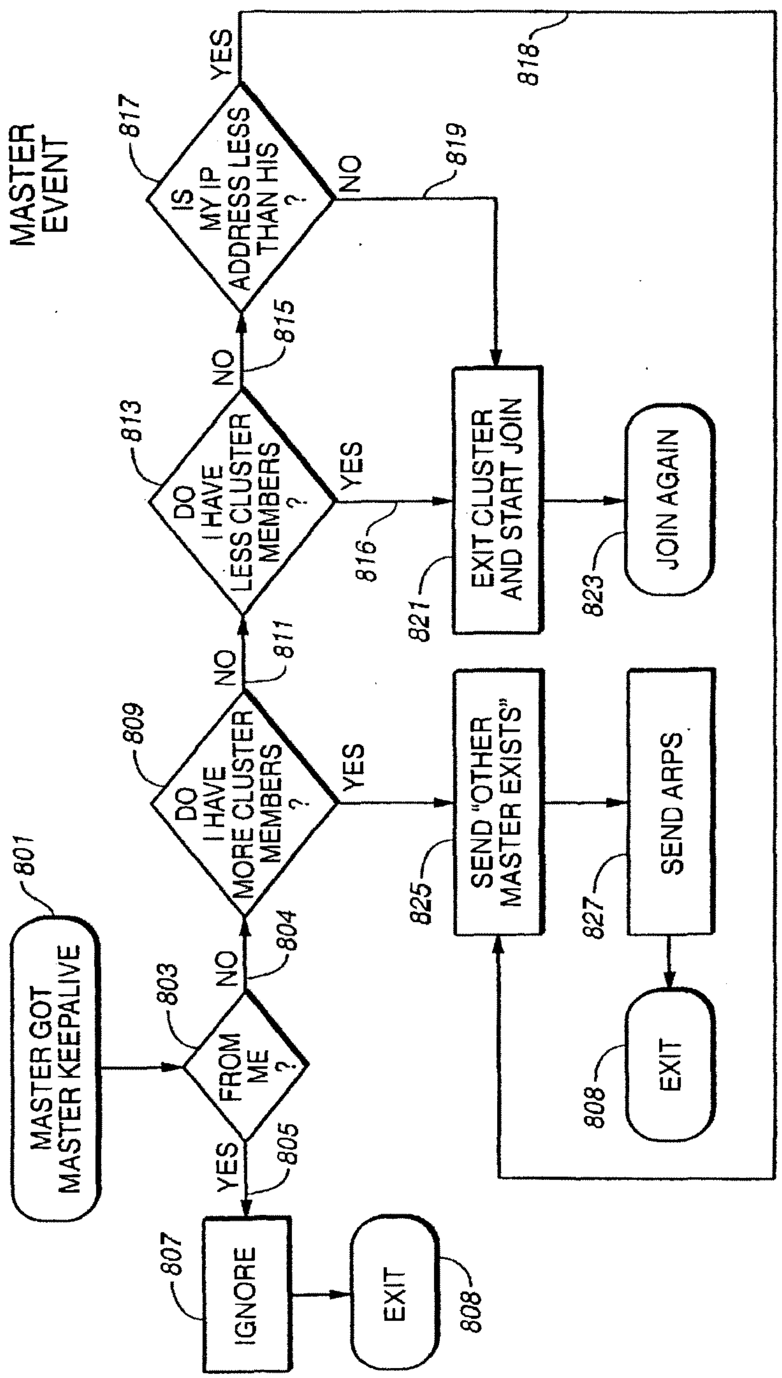


FIG._8A

VNET00221288

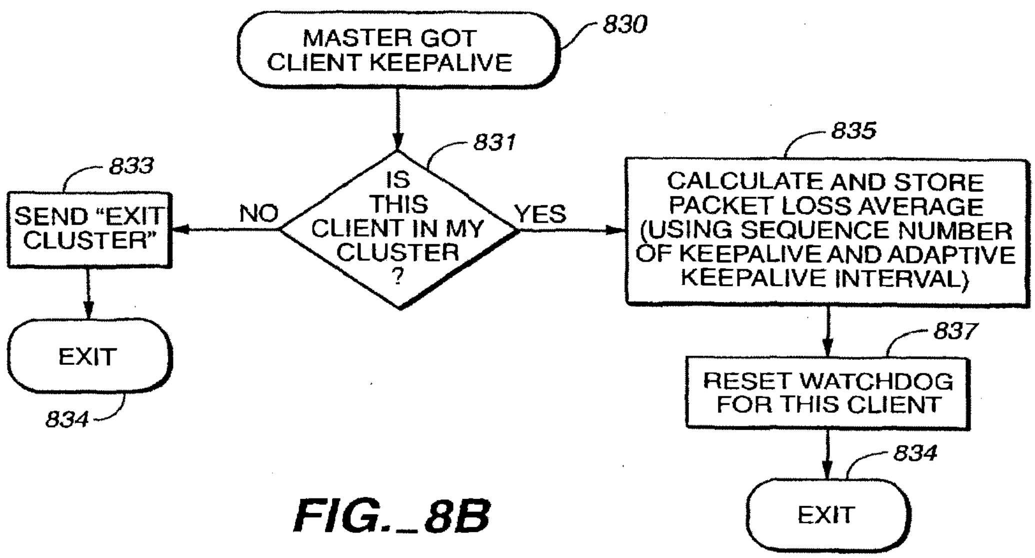

MASTER GOT CLIENT KEEPALIVE
830
IS THIS CLIENT IN MY CLUSTER ?
831
NO
YES
SEND "EXIT CLUSTER"
833
EXIT
834
CALCULATE AND STORE PACKET LOSS AVERAGE (USING SEQUENCE NUMBER OF KEEPALIVE AND ADAPTIVE KEEPALIVE INTERVAL)
835
RESET WATCHDOG FOR THIS CLIENT
837
EXIT
834

FIG._8B

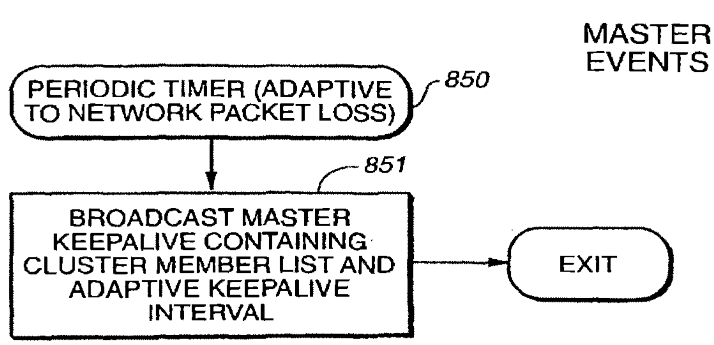

MASTER EVENTS
PERIODIC TIMER (ADAPTIVE TO NETWORK PACKET LOSS)
850
BROADCAST MASTER KEEPALIVE CONTAINING CLUSTER MEMBER LIST AND ADAPTIVE KEEPALIVE INTERVAL
851
EXIT

FIG._8C

FIG._8D

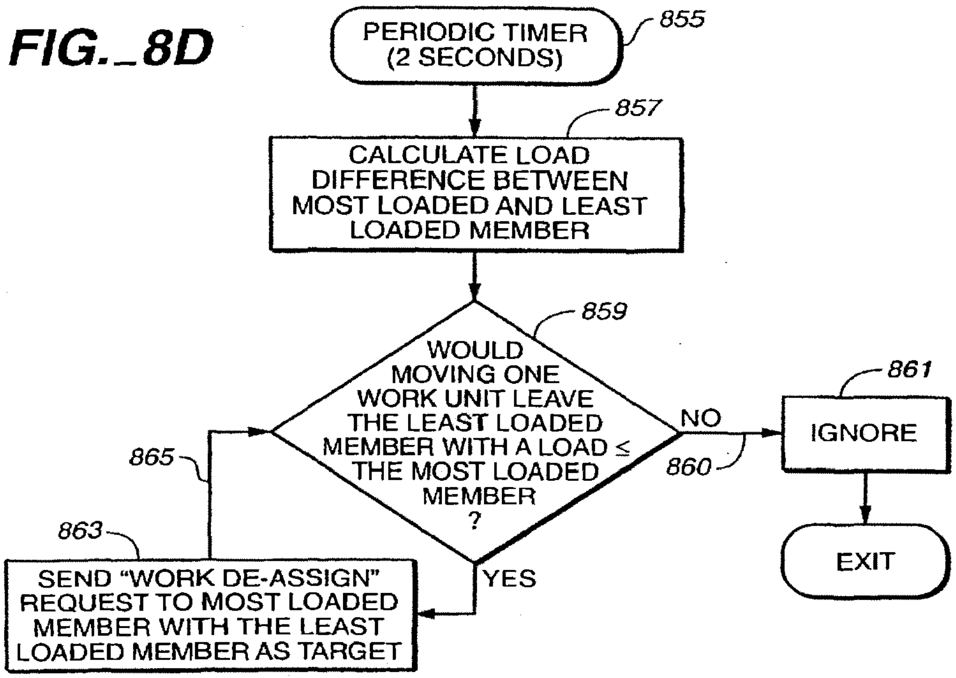


FIG._8E

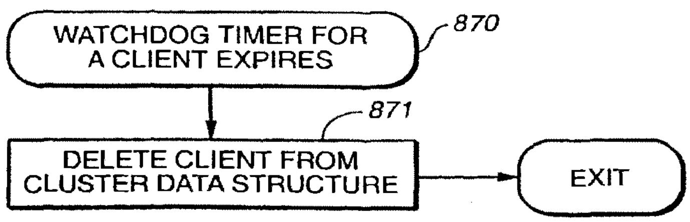
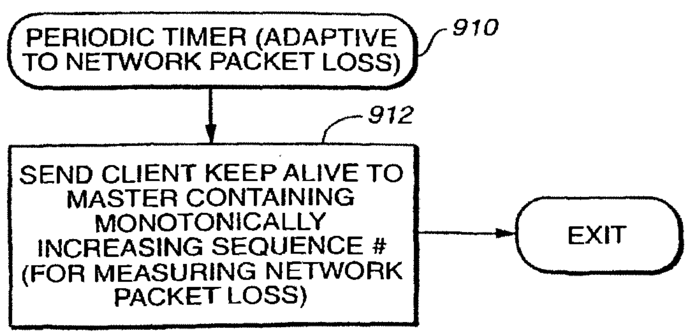


FIG._8H



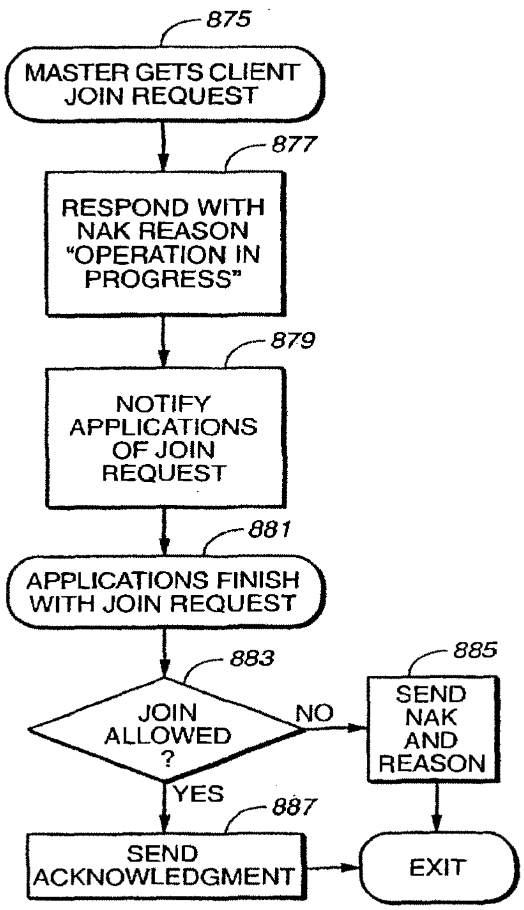


FIG._8F

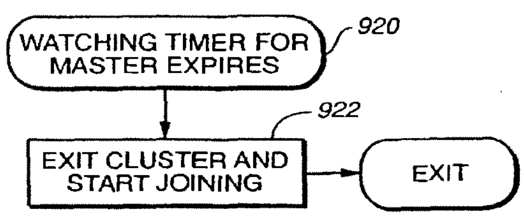


FIG._8I

CLIENT EVENTS

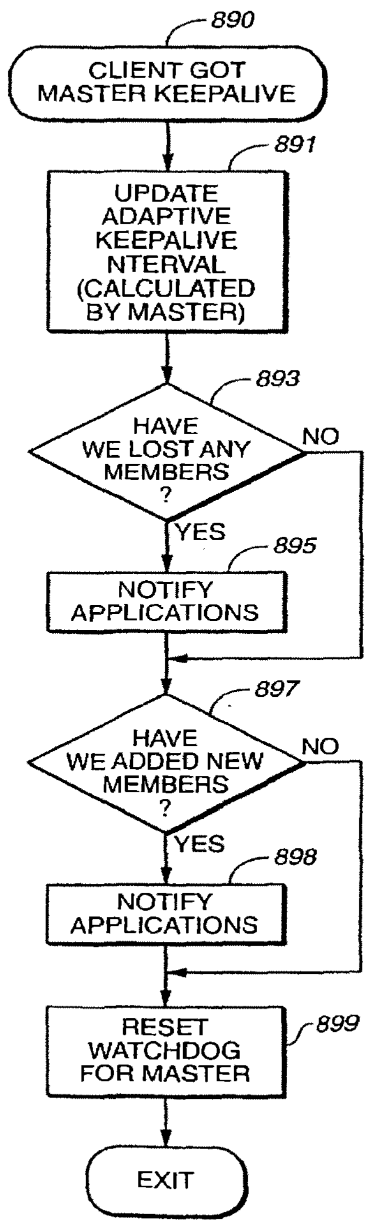


FIG._8G

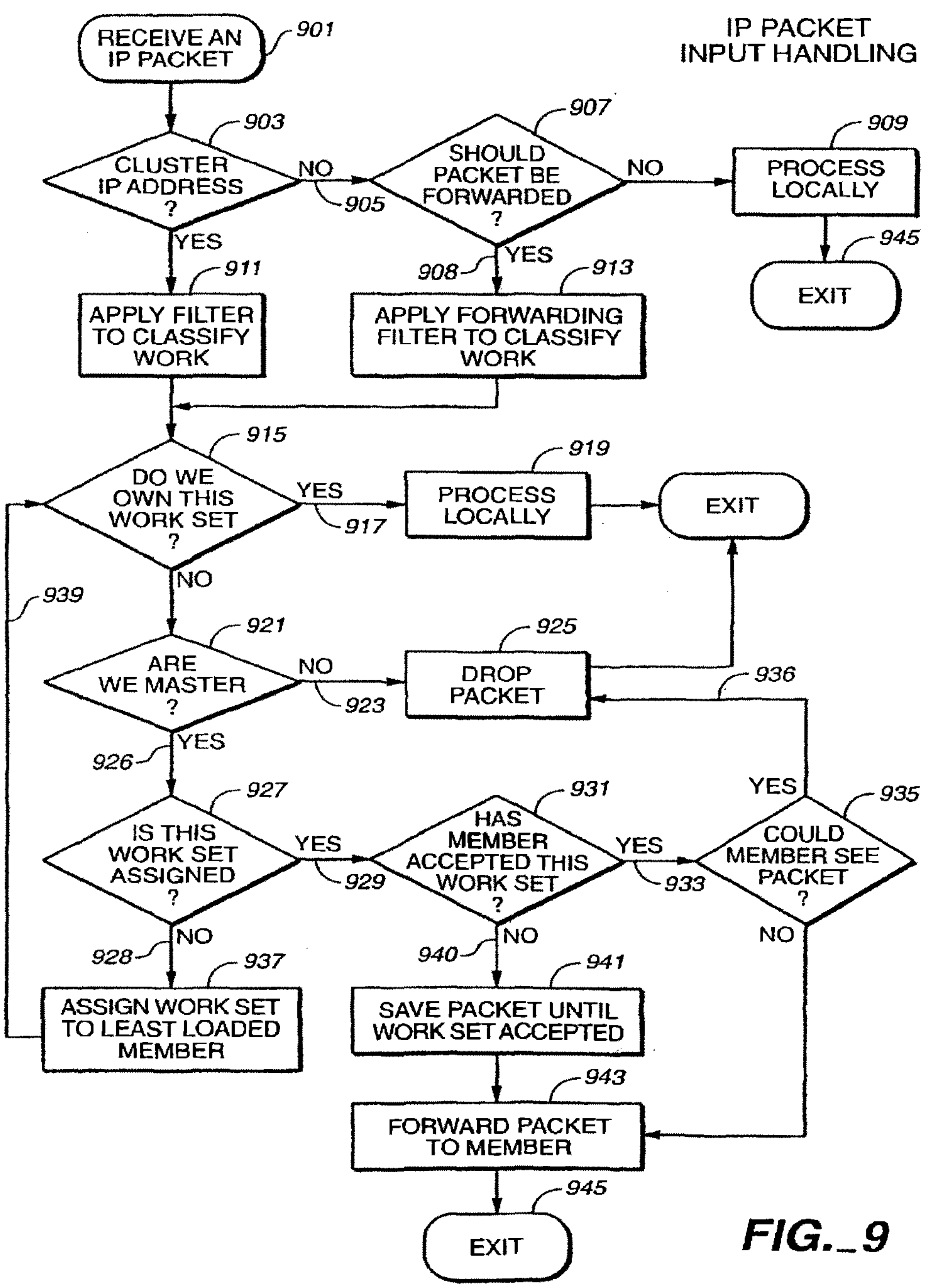

IP PACKET
INPUT HANDLING
RECEIVE AN IP PACKET
901
CLUSTER IP ADDRESS ?
903
NO
905
SHOULD PACKET BE FORWARDED ?
907
NO
PROCESS LOCALLY
909
EXIT
945
YES
YES
908
911
913
APPLY FILTER TO CLASSIFY WORK
APPLY FORWARDING FILTER TO CLASSIFY WORK
DO WE OWN THIS WORK SET ?
915
YES
917
PROCESS LOCALLY
919
EXIT
NO
939
ARE WE MASTER ?
921
NO
923
DROP PACKET
925
936
YES
926
IS THIS WORK SET ASSIGNED ?
927
YES
929
HAS MEMBER ACCEPTED THIS WORK SET ?
931
YES
933
COULD MEMBER SEE PACKET ?
935
YES
NO
NO
928
NO
940
ASSIGN WORK SET TO LEAST LOADED MEMBER
937
SAVE PACKET UNTIL WORK SET ACCEPTED
941
FORWARD PACKET TO MEMBER
943
EXIT
945

FIG._9

METHOD AND APPARATUS FOR AN INTERNET PROTOCOL (IP) NETWORK CLUSTERING SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to application Ser. No. 09/197,018 entitled "Method and Apparatus for TCP/IP load balancing in an IP Network Clustering System," concurrently filed Nov. 20, 1998, and still pending.

TECHNICAL FIELD

This invention relates to the field of Computer Systems in the general Network Communications sector. More specifically, the invention is a method and apparatus for an Internet Protocol (IP) Network clustering system.

BACKGROUND ART

As more and more businesses develop electronic commerce applications using the Internet in order to market and to manage the ordering and delivery of their products, these businesses are searching for cost-effective Internet links that provide both security and high availability. Such mission-critical applications need to run all day, every day with the network components being highly reliable and easily scalable as the message traffic grows. National carriers and local Internet Service Providers (ISPs) are now offering Virtual Private Networks (VPN)—enhanced Internet-based backbones tying together corporate workgroups on far-flung Local Area Networks (LANs)—as the solution to these requirements.

A number of companies have recently announced current or proposed VPN products and/or systems which variously support IPSec, IKE (ISAKMP/Oakley) encryption-key management, as well as draft protocols for Point-to-Point Tunneling protocol (PPTP), and Layer 2 Tunneling protocol (L2TP) in order to provide secure traffic to users. Some of these products include IBM's Nways Multiprotocol Routing Services™2.2, Bay Networks Optivity™ and Centillion™ products, Ascend Communication's MultiVPN™ package, Digital Equipment's ADI VPN product family, and Indus River's RiverWorks™ VPN planned products. However, none of these products are known to offer capabilities which minimizes delay and session loss by a controlled fail-over process.

These VPNs place enormous demands on the enterprise network infrastructure. Single points of failure components such as gateways, firewalls, tunnel servers and other choke points that need to be made highly reliable and scaleable are being addressed with redundant equipment such as "hot standbys" and various types of clustering systems.

For example, CISCO™ Inc. now offers a new product called LocalDirector™ which functions as a front-end to a group of servers, dynamically load balances TCP traffic between servers to ensure timely access and response to requests. The LocalDirector provides the appearance, to end users, of a "virtual" server. For purposes of providing continuous access if the LocalDirector fails, users are required to purchase a redundant LocalDirector system which is directly attached to the primary unit, the redundant unit acting as a "hot" standby. The standby unit does no processing work itself until the master unit fails. The standby unit uses the failover IP address and the secondary Media Access Control (MAC) address (which are the same as the primary unit), thus no Address Resolution Protocol (ARP) is required to switch to the standby unit. However, because the standby unit does not keep state information on each connection, all active connections are dropped and must be re-established by the clients. Moreover, because the "hot standby" does no concurrent processing it offers no processing load relief nor scaling ability.

Similarly, Valence™ Research Inc. (recently purchased by Microsoft® Corporation) offers a software product called Convoy Cluster™ (Convoy). Convoy installs as a standard Windows NT networking driver and runs on an existing LAN. It operates in a transparent manner to both server applications and TCP/IP clients. These clients can access the cluster as if it is a single computer by using one IP address. Convoy automatically balances the networking traffic between the clustered computers and can rebalance the load whenever a cluster member comes on-line or goes off-line. However this system appears to use a compute intensive and memory wasteful method for determining which message type is to be processed by which cluster member in that the message source port address and destination port address combination is used as an index key which must be stored and compared against the similar combination of each incoming message to determine which member is to process the message. Moreover, this system does not do failover.

There is a need in the art for an IP network cluster system which can easily scale to handle the exploding bandwidth requirements of users. There is a further need to maximize network availability, reliability and performance in terms of throughput, delay and packet loss by making the cluster overhead as efficient as possible, because more and more people are getting on the Internet and staying on it longer. A still further need exists to provide a reliable failover system for TCP based systems by efficiently saving the state information on all connections so as to minimize packet loss and the need for reconnections.

Computer cluster systems including "single-system-image" clusters are known in the art. See for example, "Scalable Parallel Computing" by Kai Hwang & Zhiwei Xu, McGraw-Hill, 1998, ISBN 0-07-031798-4, Chapters 9 & 10, Pages 453–564, which are hereby incorporated fully herein by reference. Various Commercial Cluster System products are described therein, including DEC's TruClusters™ system, IBM's SP™ system, Microsoft's Wolfpack™ system and The Berkeley NOW Project. None of these systems are known to provide efficient IP Network cluster capability along with combined scalability, load-balancing and controlled TCP fail-over.

SUMMARY OF THE INVENTION

The present invention overcomes the disadvantages of the above-described systems by providing an economical, high-performance, adaptable system and method for an IP Network cluster.

The present invention is an IP Network clustering system which can provide a highly scalable system which optimizes message throughput by adaptively load balancing its components, and which minimizes delay and packet loss especially in the TCP mode by a controlled fail-over process. No other known tunnel-server systems can provide this combined scalability, load-balancing and controlled failover.

The present invention includes a cluster apparatus comprising a plurality of cluster members, with all cluster members having the same internet machine name and IP address, and each member having a general purpose processor, a memory unit, a program in the memory unit, a display and an input/output unit; and the apparatus having a filter mechanism in each cluster member which uses a highly efficient hashing mechanism to generate an index number for each message session where the index number is used to determine whether a cluster member is to process a particular message or not. The index number is further used to designate which cluster member is responsible for processing the message and is further used to balance the processing load over all present cluster members.

The present invention further includes a method for operating a plurality of computers in an IP Network cluster which provides a single-system-image to network users, the method comprising steps to interconnect the cluster members, and assigning all cluster members the same internet machine name and IP address whereby all cluster members can receive all messages arriving at the cluster and all messages passed on by the members of the cluster appear to come from a single unit, and to allow them to communicate with each other; to adaptively designate which cluster member will act as a master unit in the cluster; and the method providing a filter mechanism in each cluster member which uses a highly efficient hashing mechanism to generate an index number for each message session where the index number is used to determine whether a cluster member is to process a particular message or not. The index number is further used to designate which cluster member is responsible for processing which message type and is further used to balance the processing load over all present cluster members.

Other embodiments of the present invention will become readily apparent to those skilled in these arts from the following detailed description, wherein is shown and described only the embodiments of the invention by way of illustration of the best mode known at this time for carrying out the invention. The invention is capable of other and different embodiments some of which may be described for illustrative purposes, and several of the details are capable of modification in various obvious respects, all without departing from the spirit and scope of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the system and method of the present invention will be apparent from the following description in which:

FIG. 1 illustrates a typical Internet network configuration.

FIG. 2 illustrates a representative general purpose computer/cluster-member configuration.

FIG. 3 illustrates a representative memory map of data contained on a related Flash Memory card.

FIG. 4 illustrates a typical IP Network cluster

FIG. 5 illustrates a general memory map of the preferred embodiment of a cluster member acting as a tunnel-server.

FIG. 6 illustrates a flow-chart of the general operation of the cluster indicating the cluster establishment process.

FIG. 7 illustrates an exemplary TCP state data structure.

FIGS. 8A–8I illustrate flow-charts depicting the events which the master processes and the events which the non-master cluster members (clients) must process.

FIGS. 9 illustrates a flow-chart depicting the normal packet handling process after establishing the cluster.

BEST MODE FOR CARRYING OUT THE INVENTION

A method and apparatus for operating an Internet Protocol (IP) Network cluster is disclosed. In the following description for purposes of explanation, specific data and configurations are set forth in order to provide a thorough understanding of the present invention. In the presently preferred embodiment the IP Network cluster is described in terms of a VPN tunnel-server cluster. However, it will be apparent to one skilled in these arts that the present invention may be practiced without the specific details, in various applications such as a firewall cluster, a gateway or router cluster, etc. In other instances, well-known systems and protocols are shown and described in diagrammatical or block diagram form in order not to obscure the present invention unnecessarily.

Operating Environment

The environment in which the present invention is used encompasses the general distributed computing scene which includes generally local area networks with hubs, routers, gateways, tunnel-servers, applications servers, etc. connected to other clients and other networks via the Internet, wherein programs and data are made available by various members of the system for execution and access by other members of the system. Some of the elements of a typical internet network configuration are shown in FIG. 1, wherein a number of client machines **105** possibly in a branch office of an enterprise, are shown connected to a Gateway/hub/tunnel-server/etc. **106** which is itself connected to the internet **107** via some internet service provider (ISP) connection **108**. Also shown are other possible clients **101, 103** similarly connected to the internet **107** via an ISP connection **104**, with these units communicating to possibly a home office via an ISP connection **109** to a gateway/tunnel-server **110** which is connected **111** to various enterprise application servers **112, 113, 114** which could be connected through another hub/router **115** to various local clients **116, 117, 118**.

The present IP Network cluster is made up of a number of general purpose computer units each of which includes generally the elements shown in FIG. 2, wherein the general purpose system **201** includes a motherboard **203** having thereon an input/output ("I/O") section **205**, one or more central processing units ("CPU") **207**, and a memory section **209** which may have a flash memory card **211** related to it. The I/O section **205** is connected to a keyboard **226**, other similar general purpose computer units **225, 215**, a disk storage unit **223** and a CD-ROM drive unit **217**. The CD-ROM drive unit **217** can read a CD-ROM medium **219** which typically contains programs **221** and other data. Logic circuits or other components of these programmed computers will perform series of specifically identified operations dictated by computer programs as described more fully below.

Flash memory units typically contain additional data used for various purposes in such computer systems. In the preferred embodiment of the present invention, the flash memory card is used to contain certain unit "personality" information which is shown in FIG. 3. Generally the flash card used in the current embodiment contains the following type of information:

Cryptographically signed kernel—**(301)**

Configuration files (such as cluster name, specific unit IP address, cluster address, routing information configuration, etc.)—**(303)**

Pointer to error message logs—**(305)**

Authentication certificate—**(307)**.

Security policies (for example, encryption needed or not, etc.)—**(309)**

The Invention

The present invention is an Internet Protocol (IP) clustering system which can provide a highly scalable system which optimizes throughput by adaptively load balancing its components, and which minimizes delay and session loss by a controlled fail-over process. A typical IP cluster system of the preferred embodiment is shown in FIG. 4 wherein the internet 107 is shown connected to a typical IP cluster 401 which contains programmed general purpose computer units 403, 405, 407, 409 which act as protocol stack processors for message packets received. The IP cluster 401 is typically connected to application servers or other similar type units 411 in the network. In this figure it is shown that there purposes of further illustration the cluster will be depicted as having three units, understanding that the cluster of the present invention is not limited to only three units. Also for purposes of illustration the preferred embodiment will be described as a cluster whose applications may be VPN tunnel protocols however it should be understood that this cluster invention may be used as a cluster whose application is to act as a Firewall, or to act as a gateway, or to act as a security device, etc.

In the preferred embodiment of the present invention, each of the cluster members is a computer system having an Intel motherboard, two Intel Pentium™ processors, a 64 megabyte memory and two Intel Ethernet controllers, and two HiFn cryptographic processors. The functions performed by each processor are generally shown by reference to the general memory map of each processor as depicted in FIG. 5. Each cluster member has an Operating System kernel 501, TCP/IP stack routines 503 and various cluster management routines (described in more detail below) 505, program code for processing application #1 507, which in the preferred embodiment is code for processing the IPSec protocol, program code for processing application #2 509, which in the preferred embodiment is code for processing the PPTP protocol, program code for processing application #3 511, which in the preferred embodiment is code for processing the L2TP protocol, and program code for processing application #4 513, which in the preferred embodiment is code space for processing an additional protocol such as perhaps a "Mobile IP" protocol. Detailed information on these protocols can be found through the home page of the IETF at "http://www.ietf.org". The following specific protocol descriptions are hereby incorporated fully herein by reference:

"Point-to-Point Tunneling Protocol—PPTP", Glen Zorn, G. Pall, K. Hamzeh, W. Verthein, J. Taarud, W. Little, Jul. 28, 1998;

"Layer Two Tunneling Protocol", Allan Rubens, William Palter, T. Kolar, G. Pall, M. Littlewood, A. Valencia, K. Hamzeh, W. Verthein, J. Taarud, W. Mark Townsley, May 22, 1998;

Kent, S., Atkinson, R., "IP Authentication Header," draft-ietf-ipsec-auth-header-07.txt.

Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol," draft-ietf-ipsec-arch-sec-07.txt.

Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)," draft-ietf-ipsec-esp-v2-06.txt.

Pereira, R., Adams, R., "The ESP CBC-Mode Cipher Algorithms," draft-ietf-ipsec-ciph-cbc-04.txt.

Glenn, R., Kent, S., "The NULL Encryption Algorithm and Its Use With IPsec," draft-ietf-ipsec-ciph-null-0.1.txt.

Madson, C., Doraswamy, N., "The ESP DES-CBC Cipher Algorithm With Explicit IV," draft-ietf-ipsec-ciph-des-expiv-02.txt.

Madson, C., Glenn, R., "The Use of HMAC-MD5 within ESP and AH," draft-ietf-ipsec-auth-hmac-md5-96-03.txt.

Madson, C., Glenn, R., "The Use of HMAC-SHA-1-96 within ESP and AH," draft-ietf-ipsec-auth-hmac-sha 196-03.txt.

Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)," draft-ietf-ipsec-isakmp-oakley-08.txt.

Maughan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)," draft-ietf-ipsec-isakmp-10.{ps,txt}.

H. K. Orman, "The OAKLEY Key Determination Protocol," draft-ietf-ipsec-oakley-02.txt.

Piper, D. "The Internet IP Security Domain of Interpretation for ISAKMP," draft-ietf-ipsec-ipsec-doi-10.txt.

Tunneling protocols such as the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) although currently only "draft" standards, are expected to be confirmed as official standards by the Internet Engineering Task Force (IETF) in the very near future, and these protocols together with the Internet Security Protocol (IPSec), provide the basis for the required security of these VPNs.

Referring again to FIG. 5, the preferred embodiment in a cluster member also contains a work assignment table 515 which contains the message/session work-unit hash numbers and the cluster member id assigned to that work-unit; a table containing the application state table for this cluster member 517; a similar application state table for the other members of the cluster 519; an area for containing incoming messages 521; and data handler routines for handling data messages from other members of the cluster 523. Those skilled in the art will recognize that various other routines and message stores can be implemented in such a cluster member's memory to perform a variety of functions and applications.

The general operation of the preferred embodiment of the IP cluster is now described in terms of (1) cluster establishment (FIG. 6) including processes for members joining the cluster and leaving the cluster; (2) master units events processing (FIGS. 8A–8F) and client units events processing (FIGS. 8G–8I); and (3) finally, normal message processing activity (FIG. 9).

Referring now to FIG. 6 the cluster establishment activity is depicted. At system start-up 601 cluster members try to join the cluster by sending (broadcasting) a "join request" message 603. This "join" message contains an authentication certificate obtained from a valid certificate authority. When the master unit receives this 'join" message it checks the certificate against a list of valid certificates which it holds and if it finds no match it simply tells him the join has failed. Note that normally when a system administrator plans to add a hardware unit to an existing cluster, he requests that his security department or an existing security certificate authority issue a certificate to the new unit and send a copy of the certificate to the master unit in the cluster. This process guarantees that someone could not illegally attach a unit to a cluster to obtain secured messages. If the master unit does match the certificate from the join message with a certificate it holds in its memory it sends an "OK to join" message. If a "OK to join" message is received 605 then this unit is designated a cluster member (client or non-master) 607. Note that each cluster member has a master-watchdog timer (i.e. a routine to keep track of whether the member got a keepalive message from the master during a certain interval, say within the last 200 milliseconds) and if the timer expires (i.e. no keepalive message from the master during the interval) it will mean that the master unit is dead 607 and the cluster member/client will try to join the cluster again (611). Another event that will cause the cluster member/client 607 to try to join up again is if it gets an "exit request" message (i.e. telling it to "leave the cluster") **609** If the member sending out the join request message (**603**) does not get a "OK to join" message **613** the member sends out (broadcasts) packets offering to become the master unit **615**. If the member gets a "other master exists" message **617** the member tries to join again **603**. If after the member sends out the packets offering to become the master, he gets no response for 100 milliseconds **619** he sends broadcast Address Resolution Protocol (ARP) responses to tell anyone on the network what Ethernet address to use for the cluster IP address **621** and now acts as the cluster master unit **623**. If in this process the cluster member got no indication that another master exists (at **617**) and now thinking it is the only master **623** but yet gets a message to "exit the cluster" **641** the member must return to try to join up again **642**. This could happen for example, if this new master's configuration version was not correct. He would return, have an updated configuration and attempt to rejoin. Similarly, if this member who thinks he is the new master **623** gets a "master keepalive" message **625** (indicating that another cluster member thinks he is the master unit) then he checks to see if somehow the master keepalive message was from him **627** (normally the master doesn't get his own keepalive messages but it could happen) and if so he just ignores the message **639**. If however the master keepalive message was not from himself **629** it means there is another cluster member who thinks he is the master unit and somehow this "tie" must be resolved. (This tie breaker process is described in more detail below with respect to "Master event" processing). If the tie is resolved in favor of the new cluster member who thinks he is the master **635** he sends an "Other master exists" message to the other master and once again sends broadcast Address Resolution Protocol (ARP) responses to tell anyone on the network what Ethernet address to use for the cluster IP address **637** (because that other master could have done the same). If this new cluster member who thinks he is the master loses the tie-breaker **633** then he must go and join up again to try to get the cluster stabilized. This process produces a single cluster member acting as the master unit and the other cluster members understanding they are merely members.

Master Unit Events Processing

After a cluster has formed, there are various events that occur which the master unit must address. How these are handled in the preferred embodiment are now described with reference to FIGS. **8A**–**8F**. Referring to FIG. **8A** the first master unit event describes the "tie-breaker" process when two cluster members claim to be the "master" unit. Recalling from above that the master normally does not receive his own "keepalive" message so that if a master gets a "master keepalive" message **801** it likely indicates that another cluster member thinks he is the master. In the preferred embodiment, the "master keepalive" message contains the cluster member list, the adaptive keepalive interval (which is described in more detail below) and the current set of work assignments for each member which is used only for diagnostic purposes. So when a master gets a master keepalive message **801** he first asks "is it from me?" **803** and if so he just ignores this message **807** and exits **808**. If the master keepalive message is not from this master unit **804** then the "tie-breaker" process begins by asking "Do I have more cluster members than this other master?" **809** If this master does then he sends a "other master exists" message **825** telling the other master to relinquish the master role and rejoin the cluster. The remaining master then once again sends broadcast Address Resolution Protocol (ARP) responses to tell anyone on the network what Ethernet address to use for the cluster IP address **827** and exits **808**. If the current master does not have more cluster members than this other master **811** he asks "do I have less cluster members than the other master?" **813** and if so **816** he must give up the master role to the other one by exiting the cluster **821** and rejoining the cluster as a member/non-master **823**) exiting to **601** in FIG. **6**. If the current master does not have less members than the other master **815** (which indicates they both have the same number) then the final tie-breaker occurs by asking "is my IP address less than his?" **817** and if so then again the current master wins the tie-breaker **818** and sends the "other master exists" message as before **825** If however he loses this final tie-breaker **819** then he exits the cluster to rejoin as a non-master member **821**.

Referring now to FIG. **8B** another master event occurs when the master gets a "client keepalive message" (that is one from a non-master cluster member) **830**. The master asks "is this client in my cluster?" **831** and if not the master sends the client an "exit cluster" message **833** telling the client to exit from this cluster. If the client is from this master's cluster the master calculates and stores a packet loss average value using the sequence number of the client keepalive message and the calculated adaptive keepalive interval. **835** The master then resets the watchdog timer for this client **837**. The watchdog timer routine is an operating system routine that checks a timer value periodically to see if the failover detection interval has elapsed since the value was last reset and if so the watchdog timer is said to have expired and the system then reacts as if the client in question has left the cluster and reassigns that clients work-load to the remaining cluster members.

As indicated above, the master periodically sends out a master keepalive message containing the cluster member list, the adaptive keepalive interval (which is described in more detail below) and the current set of work assignments for each member which is used only for diagnostic purposes. (See FIG. **8C**). In addition, the master periodically (in the preferred embodiment every 2 seconds) checks the load-balance of the cluster members. In FIG. **8D** when the timer expires **855** the master calculates the load difference between most loaded (say "K") and least loaded (say "J") cluster member **857** and then asks "would moving 1 work unit from most loaded (K) to least loaded (J) have any effect?" that is, if K>J is K−1≧J−1? **859**. If so then the master sends a "work de-assign" request to the most loaded member with the least loaded member as the target recipient **863** and then the master checks the load numbers again **865**. If the result of moving 1 work unit would not leave the least loaded less than or equal to the most loaded **860** then the master makes no reassignments and exits **861**.

Another master event occurs when a watchdog timer for a client/cluster member expires wherein the master deletes that client from the cluster data list and the deleted unit's work goes into a pool of unassigned work to get reassigned normally as the next message arrives. (See FIG. **8E**).

Referring now to FIG. **8F** another master event in the preferred embodiment occurs when the master gets a client join request message **875**. The master initially tells the client to wait by sending a NAK with an "operation in progress" reason. **877** The master then notifies the applications that are present that a client is trying to join the cluster as some applications want to know about it. **879**. For example if IPSec is one of the applications then IPSec may want to validate this client before agreeing to let it join the cluster. If any application rejects the join request the master sends a NAK with the reason **855** and exits. If all applications approve the join request the master sends an ACK and the join proceeds as normal. **887**.

Client Cluster Member Events

The non-master cluster members (clients) must also send keepalive messages and monitor the watchdog timer for the master. Referring now to FIG. 8G when a client gets a master keepalive message **890** it updates its adaptive keepalive interval **891**, and checks the list of cluster members to see if any members have been lost **893**. If so this client notifies its applications that a cluster member has departed **895** (for example, IPSec wants to know). The client also checks to see if any members have been added to the cluster **897** and if so notifies the applications **898** and finally resets the watchdog timer for monitoring the master **899** and exits. Each client also has a periodic timer which is adaptive to the network packet loss value sent by the master which requires the client to send a client keepalive message (containing a monotonically increasing numeric value) to the master periodically (See FIG. 8H). Also each client has a master watchdog timer it must monitor and if it expires the client must exit the cluster and send a new join message to re-enter the cluster. (See FIG. 8I).

Normal IP Packet Processing

In order for a cluster member to correctly process only its share of the workload, one of three methods is used:

1. The MAC address of the master is bound to the cluster IP address (using the ARP protocol). The master applies the filtering function (described in more detail below) to classify the work and forward each packet (if necessary) to the appropriate cluster member.

2. A cluster-wide Unicast MAC address is bound to the cluster IP address (using the ARP protocol). Each cluster member programs its network interface to accept packets from this MAC destination address. Now each cluster member can see all packets with the cluster IP address destination. Each member applies the filtering function and discards packets that are not part of its workload.

3. method 2 is used but with a Multicast MAC address instead of a Unicast MAC address. This method is required when intelligent packet switching devices are part of the network. These devices learn which network ports are associated with each Unicast MAC address when they see packets with a Unicast MAC destination address, and they only send the packets to the port the switching device has determined is associated with that MAC address (only 1 port is associated with each Unicast MAC address). A Multicast MAC address will cause the packet switching device to deliver packets with the cluster IP destination address to all cluster members.

In the preferred embodiment, there is a mechanism for designating which cluster member is to process a message and allow the other members to disregard the message without inadvertently sending a "reset" message to the originating client. The preferred embodiment makes use of a "filter" process in each cluster member which calculates a hash function using certain fields of the incoming message header. This hash calculation serves as a means of both assigning a work unit number to a message and assigning a work unit to a particular cluster member for processing. This technique allows a cluster member to tell whether the incoming message must be processed by it, therefore the possibility of an inadvertent "reset" message is precluded. It is noted that other solutions to this problem of "how to get the work to the right member of the cluster with minimum overhead" could include a hardware filter device sitting between the network and the cluster wherein the hardware filter would do the member assignment and load balancing function. Note that since all cluster members have the same MAC address, all cluster members get all messages and the way they tell whether they must process the message further is to calculate the work unit number using the hashing method shown above and then to check the resulting work unit number against their work load table to see if it is assigned to them. If not they dump the message from their memory. This is a fast and efficient scheme for dumping messages that the units need not process further and yet it provides an efficient basis for load-balancing and efficient fail-over handling when a cluster member fails.

The normal processing of IP packets is described with reference to FIG. 9. Upon the receipt of a packet **901** a determination is made as to whether the packet is addressed to a cluster IP address **903** or not. If not **905** then it is determined if the IP address is for this cluster member and if so it is processed by the IP stack locally **909**. If the packet is to be forwarded (here the system is acting like a router) **908** a forward filter is applied in order to classify the work **913**.

This designates whether the packet is for normal work for the cluster clients or is forwarding work. If at step **903** where the address was checked to see if it was a cluster IP address, the answer was yes then a similar work set filter is applied **911** wherein the IP source and destination addresses are hashed modulo 1024 to produce an index value which is used for various purposes. This index value calculation (the processing filter) is required in the current embodiment and is described more fully as follows;

Basically the fields containing the IP addresses, IP protocol, and TCP/UDP port numbers, and if the application is L2TP, the session and tunnel ID fields are all added together (logical XOR) and then shifted to produce a unique "work unit" number between 0 and 1023.

For example, in the preferred embodiment the index could be calculated as follows:

```
/*
 * Sample Cluster Filtering function
 */
static int Cluster_Filtering_Function(voil*Packet, int Forwarding)
{
   struct ip *ip = (struct ip *)Packet;
   int i, length;
   /*
    * Select filtering scheme based on whether or not we are
forwarding this packet
    */
    if (Forwarding) {
        /*
         * Filter Forwarded packets on source & destination
IP address
        i = ip->ip_dst.s_addr;
        i ^=ip->ip_src.s_addr;
    } else {
        /*
         * Not forwarding: Put in the IP source address
         */
        i = ip->ip_src.s_addr;
        /*
         * Get the packet header length and dispatch on protocol
         */
        length = ip->ip_hl << 2;
        if (ip->ip_p==IPPROTO_UDP) {
            /*
             * UDP: Hash on UDP Source Port and Source IP
Address
             */
            i ^=((struct udphdr *)((char *)ip + length))->uh_sport;
        } else if (ip->ip_p==IPPROTO_TCP) {
            /*
```

-continued

```
                * Hash on the TCP Source Port and Source IP Address
                */
               i ^=((struct tcphdr *)((char *)ip + length))->th_sport;
            } else {
               /*
                * Any other protocol: Hash on the Destination and
Source IP Addresses
                */
               i ^=ip->ip_dst.s_addr;
            }
        }
        /*
         * Collapse it into a work-set number
         */
        return(IP_CLUSTER_HASH(i));
    }
```

Referring again to FIG. 9, and having the work set index value calculated each member making this calculation uses the index value as an indirect pointer to determine for this work set if it is his assigned work set **915**, **917**. If the index value does not indicate that this work set has been assigned to this cluster member, if this cluster member is not the cluster master, then the packet is simply dropped by this cluster member **921**, **923**, **925**. If on the other hand this cluster member is the master unit **926** then the master must check to see if this work set has been assigned to one of the other cluster members for processing **927**. If it has been assigned to another cluster member **929** the master checks to see if that cluster member has acknowledged receiving the assignment **931** and if so the master checks to see if he was in the multicast mode or unicast/forwarding mode **933**, **935**. If he is in the unicast or multicast mode the master drops the packet because the assigned cluster member would have seen it **936**. If however, the master was in the forwarding mode the master will forward the packet to the assigned member for processing **943**. If the assigned cluster member has not acknowledged receiving the assignment yet **940** then save the packet until he does acknowledge the assignment **941** and then forward the packet to him to process **943**. If when the master checked to see if this work set had been assigned at **927** the answer is no **928** then the master will assign this work set to the least loaded member **937** and then resume its previous task **939** until the assigned member acknowledges receipt of the assignment as described above. If work is for this member, the packet is passed on to the local TCP/IP stack.

State Maintenance

RFC 1180 A TCP/IP Tutorial, T. Socolofsky and C. Kale, January 1991 generally describes the TCP/IP protocol suite and is incorporated fully herein by reference. In the present invention, a key element is the ability to separate the TCP state into an essential portion of the state and a calculable portion of the state. For example, the state of a TCP message changes constantly and accordingly it would not be practical for a cluster member to transfer all of this TCP state to all of the other members of the cluster each time the state changed. This would require an excessive amount of storage and processing time and would essentially double the traffic to the members of the cluster. The ability of the member units to maintain the state of these incoming messages is critical to their ability to handle the failure of a member unit without requiring a reset of the message session. FIG. 7 depicts the preferred embodiment's definition of which elements of the TCP state are considered essential and therefore must be transferred to each member of the cluster **701** when it changes, and which elements of the TCP state are considered to be calculable from the essential state **703** and therefore need not be transferred to all members of the cluster when it changes. The TCP Failover State **700** in the present embodiment actually comprises three portions, an Initial State portion **702** which only needs to be sent once to all cluster members; the Essential State Portion **701** which must be sent to all cluster members for them to store when any item listed in the Essential portion changes; and the Calculable State portion **703** which is not sent to all members. The data to the right of the equals sign ("=") for each element indicates how to calculate that elements value whenever it is needed to do so.

Failover Handling

As indicated above, the preferred embodiment of the IP cluster apparatus and method also includes the ability to monitor each cluster member's operation in order to manage the cluster operation for optimal performance. This means insuring that the cluster system recognize quickly when a cluster member becomes inoperative for any reason as well as have a reasonable process for refusing to declare a cluster member inoperative because of packet losses which are inherent in any TCP/IP network. This monitoring process is done in the preferred embodiment by a method whereby each non-member cluster member keeps a "master watchdog timer" and the master keeps a "client watchdog timer" for all cluster members. These watchdog timers are merely routines whereby the cluster member's OS periodically checks a "watchdog time-value" to see if it is more than "t" time earlier than the current time (that is, to see if the watchdog time value has been reset within the last "t" time). If the routine finds that the difference between the current time and the watchdog time value is greater than "t" time then it declares the cluster member related to the watchdog timer to be inoperative. These watchdog time values are reset whenever a cluster member sends a "keepalive" packet (sometimes called a "heartbeat" message) to the other members.

Generally a "keepalive" message is a message sent by one network device to inform another network device that the virtual circuit between the two is still active. In the preferred embodiment the master unit sends a "master keepalive" packet that contains a list of the cluster members, an "adaptive keepalive interval" and a current set of work assignments for all members. The non-master cluster members monitor a Master watchdog timer to make sure the master is still alive and use the "adaptive keepalive interval" value supplied by the master to determine how frequently they (the non-master cluster members) must send their "client keepalive" packets so that the master can monitor their presence in the cluster. The "client keepalive" packets contain a monotonically increasing sequence number which is used to measure packet loss in the system and to adjust the probability of packet loss value which is used to adjust the adaptive keepalive interval. Generally these calculations are done as follows in the preferred embodiment, however it will be understood by those skilled in these arts that various programming and logical circuit processes may be used to accomplish equivalent measures of packet loss and related watchdog timer values.

Each client includes a sequence number in its "client keepalive" packet. When the master gets this keepalive packet for client "x" he makes the following calculations:

$$S_\Delta=[\text{this sequence number}]-[\text{last sequence number}]-1$$

This value S_Δ is typically=0 or 1 and represents the number of dropped packets between the last two keepalive messages, or the current packet loss for client "x".

This value is then used in an exponential smoothing formula to calculate current average packet loss "P" as follows;

$$P_{new}=P_{old}X[127/128]+S_NX[1/128]$$

This P_{new} then represents the probability of a lost packet, and

P^n (P to the nth power) would represent the probability of getting "n" successive packet losses. And $1/P^n$ would be how often we would lose "n" packets in a row.

So "n" is defined as the number of lost packets per interval, and P^n then is the probability of losing "n" packets in an interval. Obviously if we lose more than some number of packets in a given interval the cluster member is either malfunctioning, inoperative or the network is having problems. In the preferred embodiment we assume "n" is a number between 2 and 20 and calculate its value adaptively as follows

We call the interval "K" and set $1/K=n\ P^n$. By policy we set K=3600 (which is equivalent to a period of 1 week) and then calculate the smallest integer value of "n" for which $n\ P^n. <1/3600$. In the preferred embodiment this is done by beginning the calculation with n=2 and increasing n by 1 iteratively until the condition is met. The resulting value of "n" is the adaptive keepalive interval which the master then sends to all of the cluster members to use in determining how often they are to send their "Client keepalive" messages.

Having described the invention in terms of a preferred embodiment, it will be recognized by those skilled in the art that various types of general purpose computer hardware may be substituted for the configuration described above to achieve an equivalent result. Similarly, it will be appreciated that arithmetic logic circuits are configured to perform each required means in the claims for processing internet security protocols and tunneling protocols; for permitting the master unit to adaptively distribute processing assignments for incoming messages and for permitting cluster members to recognize which messages are theirs to process; and for recognizing messages from other members in the cluster. It will be apparent to those skilled in the art that modifications and variations of the preferred embodiment are possible, which fall within the true spirit and scope of the invention as measured by the following claims.

What is claimed is:

1. An Internet Protocol (IP) Network cluster apparatus comprising:

a. a plurality of cluster members with all cluster members being addressable by a single dedicated Internet machine name and IP address for the cluster, each cluster member comprising a computer system having a processor, a memory, a program in said memory, a display screen and an input/output unit;

b. a filter mechanism in each cluster member, the filter mechanism using a hashing mechanism to generate an index number for each message session received by the cluster member, the index number being used to indicate to which workset a message belongs, worksets being assigned to cluster members to balance processing load, each cluster member checking whether the workset has been assigned to it in order to determine whether the cluster member must process the message received or ignore it.

2. The apparatus of claim 1 further comprising an assignment mechanism in each cluster member, for use by a cluster member designated as a master unit, the assignment mechanism used when a message of an unassigned message session is received by the master unit, the assignment mechanism using the index number calculated by the filter mechanism to assign sets of message sessions to cluster members for further processing in order to load balance processing of incoming messages.

3. The apparatus of claim 1 further comprising a first program code mechanism in each of the plurality of cluster members configured to save state for each message session including TCP state.

4. The apparatus of claim 3 further comprising a second program code mechanism in each of the plurality of cluster members configured to transfer an essential portion of the saved state for each message session to each of the other cluster members, whenever required.

5. The apparatus of claim 4 further comprising a third program code mechanism in each of the plurality of cluster members configured to permit a cluster member acting as a master unit to recognize an equipment failure in one of the other members in the cluster, to reassign the work of the failed cluster member to remaining members in the cluster thereby rebalancing the processing load and maintaining the message sessions.

6. The apparatus of claim 5 further comprising a fourth program code mechanism in each of the plurality of cluster members configured to permit units which are not acting as the master unit to recognize an equipment failure in the master unit, to immediately and cooperatively designate one of the remaining cluster members as a new master unit, the new master unit to reassign the work of the failed cluster member to remaining cluster members thereby rebalancing the processing load and maintaining the message sessions.

7. The apparatus of claim 1 wherein the memory of each of the cluster members includes a flash memory card containing a program code mechanism which describes the personality of the cluster member including its cluster address.

8. A method for operating a plurality of computers in an Internet Protocol (IP) Network cluster, the cluster providing a single-system-image to network users, the method comprising the steps of;

a. providing a plurality of cluster members, each cluster member comprising a computer system having a processor, a memory, a program in said memory, a display screen and an input/output unit;

b. interconnecting the cluster members together, and assigning all cluster members a same internet machine name and a same IP address whereby a message arriving at the cluster will be recognized by the appropriate member in the cluster and an output from any cluster member will be recognized as coming from the cluster, and whereby the cluster members can communicate with each other; and

c. providing a filter mechanism in each cluster member, the filter mechanism using a hashing mechanism to generate an index number for each message session received by the cluster member, the index number being used to indicate to which workset a message belongs, worksets being assigned to cluster members to balance processing load, each cluster member checking whether the workset has been assigned to it in order to determine whether the cluster member must process the message received or ignore it.

9. The method of claim 8 further comprising an assignment mechanism in each cluster member, for use by a cluster member designated as a master unit, the assignment mechanism used when a message of an unassigned message session is received by the master unit, the assignment mechanism using the index number calculated by the filter mechanism to assign sets of message sessions to cluster members for further processing in order to load balance processing of incoming messages.

10. The method of claim 8 comprising the additional step of each cluster member saving state for each message session connection including TCP state, and for segregating this state into an essential state portion and a non-essential state portion.

11. The method of claim 10 comprising the additional step of each cluster member transferring to each other cluster member the saved essential state portion for message sessions for which that cluster member is responsible, such transfer to be made whenever the essential portion of the state changes, whereby all cluster members maintain essential state for all message session connections.

12. The method of claim 11 comprising the additional step of each cluster member recognizing the equipment failure of one of the cluster members, immediately reassigning a task of being the master if it is the master unit that failed, the master unit reassigning the work which was assigned to the failed cluster member, rebalancing the load on the remaining tunnel-servers.

13. An Internet Protocol (IP) network cluster apparatus comprising:

a. a plurality of interconnected cluster members, each cluster member comprising a computer system having a processor, a memory, a program in said memory, a display screen and an input/output unit;

b. means in each of the plurality of cluster members for recognizing other members of the plurality of cluster members which are connected together and cooperating with the other members to adaptively designate a master unit; and

c. means for generating an index number for each message session received by a cluster member, the index number being used to indicate whether the cluster member must process the message received or ignore it.

14. The apparatus of claim 13 further comprising means in each of the plurality of cluster members for saving essential state for each message session.

15. The apparatus in claim 14 further comprising means in each of the plurality of cluster members for periodically transferring the saved essential state for each message session to each of the other members in the cluster.

16. The apparatus of claim 15 further comprising means in each of the plurality of cluster members for permitting a cluster member acting as a master unit to recognize an equipment failure in one of the other cluster members, and for reassigning work of the failed cluster member to remaining members in the cluster thereby rebalancing the processing load and maintaining message session connections, and for permitting cluster members which are not acting as a master unit to recognize an equipment failure in the master unit, to immediately and cooperatively designate one of the remaining cluster members as a new master unit, the new master unit to reassign work of the failed cluster member to remaining members in the cluster thereby rebalancing the processing load and maintaining message session connections.

* * * * *

US005905859A

United States Patent [19]

Holloway et al.

[11] Patent Number: 5,905,859

[45] Date of Patent: May 18, 1999

[54] **MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS**

[75] Inventors: **Malcolm H. Holloway**, Durham; **Thomas Joseph Prorock**, Raleigh, both of N.C.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **08/775,536**

[22] Filed: **Jan. 9, 1997**

[51] **Int. Cl.**[6] **G06F 11/00**

[52] **U.S. Cl.** **395/187.01**

[58] **Field of Search** 395/187.01, 186, 395/185.09, 200.53, 200.54, 200.59, 200.55; 380/3, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

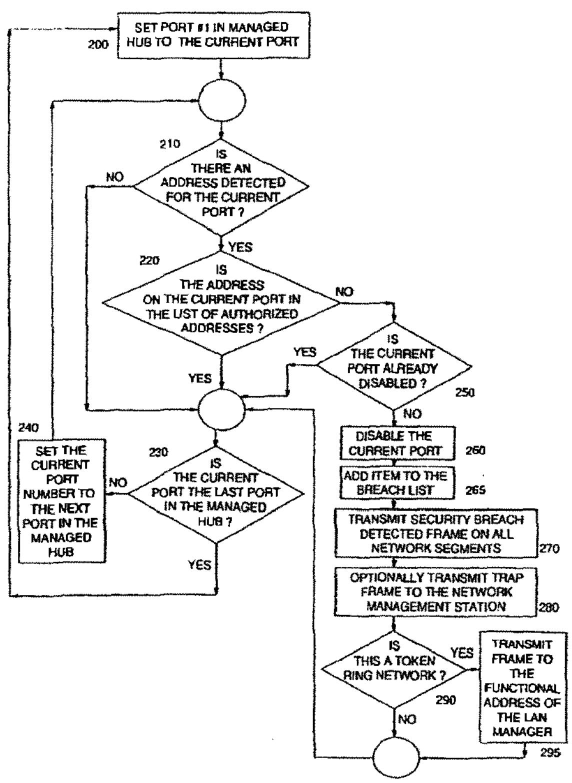
4,930,159	5/1990	Kravitz et al.	380/23
5,177,788	1/1993	Schanning et al.	380/23
5,305,385	4/1994	Schanning et al.	380/49
5,311,593	5/1994	Carmi	380/23
5,337,309	8/1994	Faulk, Jr.	370/60
5,414,833	5/1995	Hershey et al.	395/575
5,421,024	5/1995	Faulk, Jr. et al.	395/800
5,440,723	8/1995	Arnold et al.	395/183.14
5,495,580	2/1996	Osman	395/187.01
5,537,099	7/1996	Liang	340/825.07
5,606,668	2/1997	Shwed	395/187.01
5,615,340	3/1997	Dai et al.	395/187.01
5,727,146	3/1998	Savoldi et al.	395/187.01

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Scott T. Baderman
Attorney, Agent, or Firm—John J. Timar

[57] **ABSTRACT**

An apparatus and method for providing security against intrusion in the managed devices of a campus LAN network is provided. A managed hub discovers each interconnect device in the network that supports the security feature and maintains an interconnect device list of such devices, which may include token ring switches, Ethernet switches, bridges and routers. The managed hub detects an intrusion by an unauthorized address on one of its ports and notifies the interconnect devices of the intrusion by transmitting a security breach detected frame. After each interconnect device sets a filter on its respective ports against the intruding unauthorized address and sends a filter set frame to the managed hub, the port in the managed hub where the security intrusion occurred is reenabled.

35 Claims, 15 Drawing Sheets



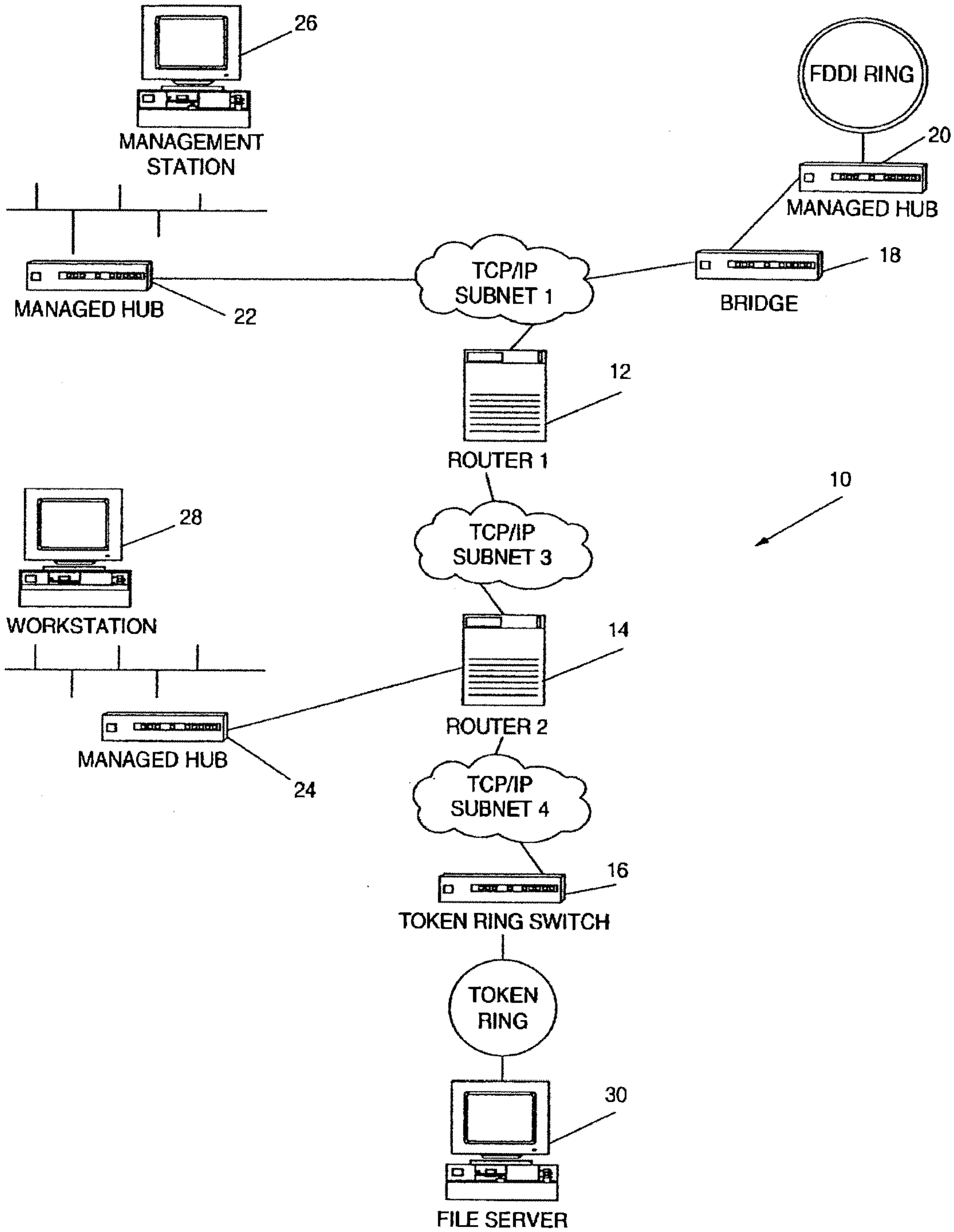

26
MANAGEMENT STATION
FDDI RING
20
MANAGED HUB
TCP/IP SUBNET 1
18
BRIDGE
MANAGED HUB
22
12
ROUTER 1
10
28
TCP/IP SUBNET 3
WORKSTATION
14
ROUTER 2
MANAGED HUB
24
TCP/IP SUBNET 4
16
TOKEN RING SWITCH
TOKEN RING
30
FILE SERVER

FIG. 1

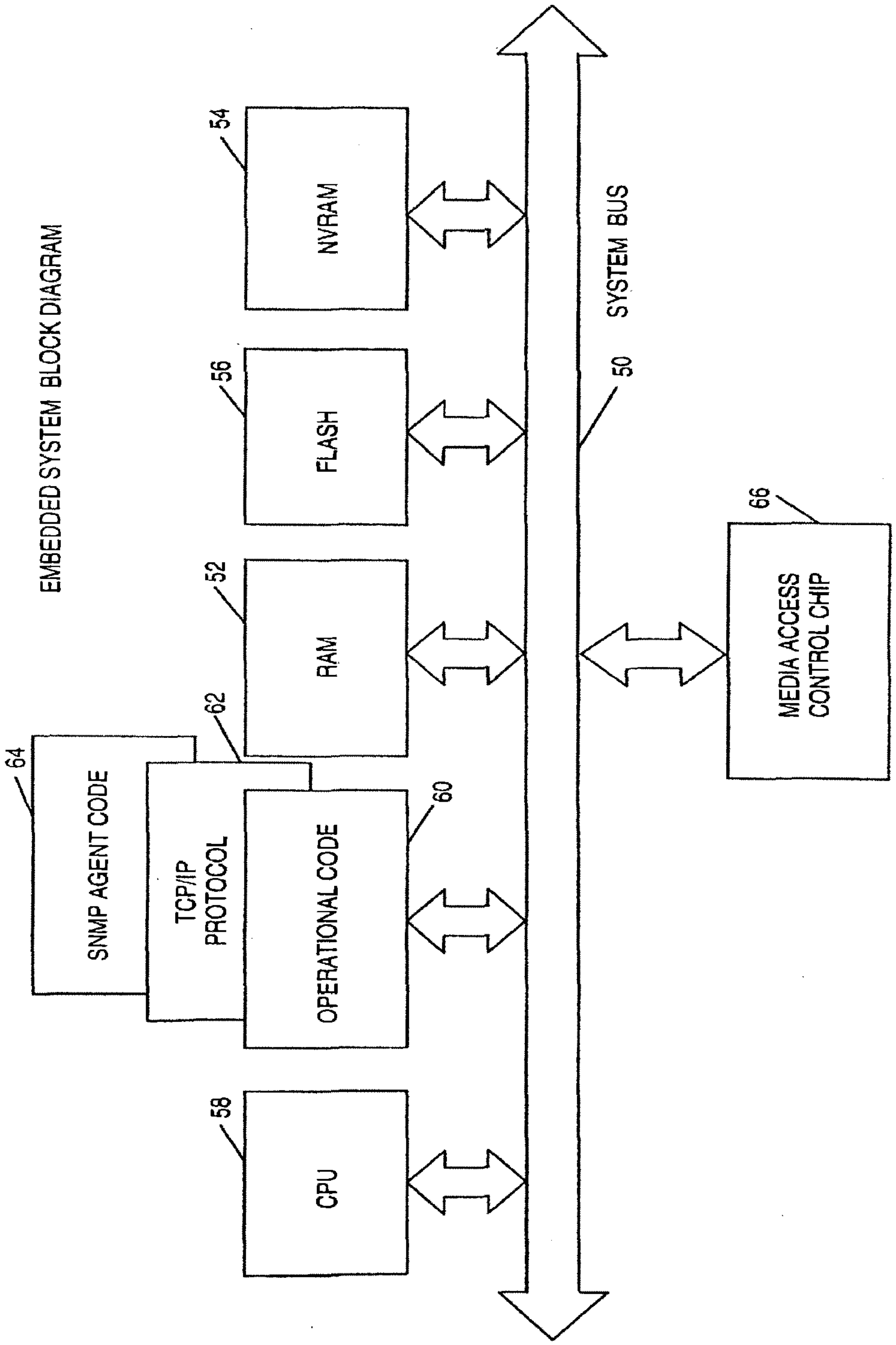

EMBEDDED SYSTEM BLOCK DIAGRAM
NVRAM
54
FLASH
56
RAM
52
OPERATIONAL CODE
60
TCP/IP
PROTOCOL
62
SNMP AGENT CODE
64
CPU
58
SYSTEM BUS
50
MEDIA ACCESS
CONTROL CHIP
66

FIG. 2

NETWORK MANAGEMENT STATION BLOCK DIAGRAM

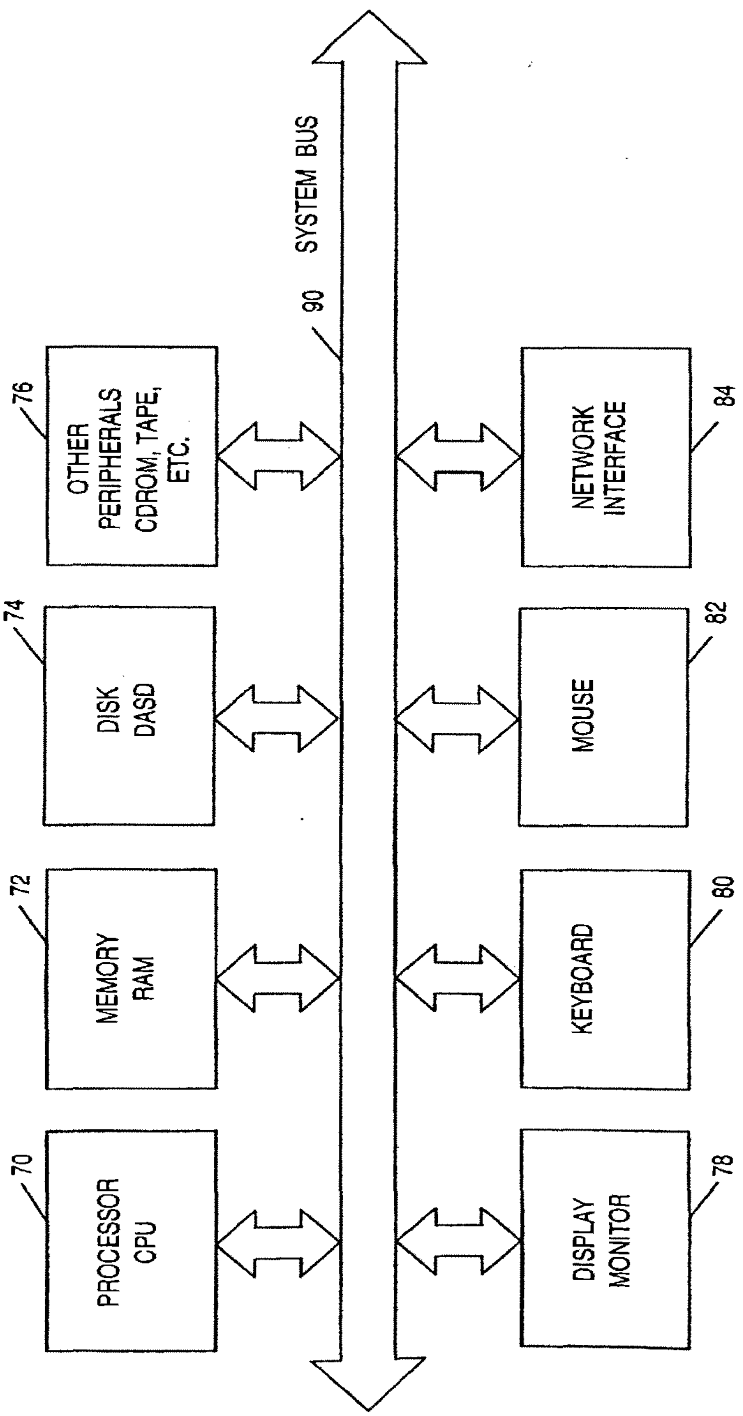


FIG. 3

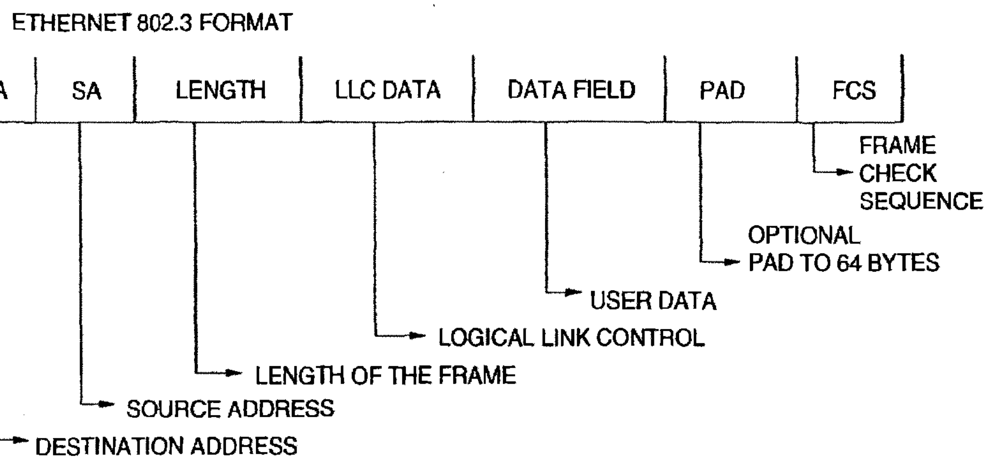


FIG. 4A

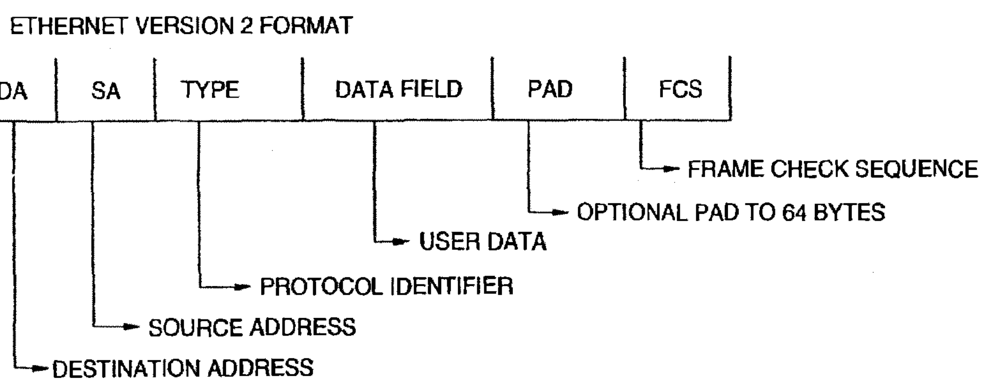


FIG. 4B

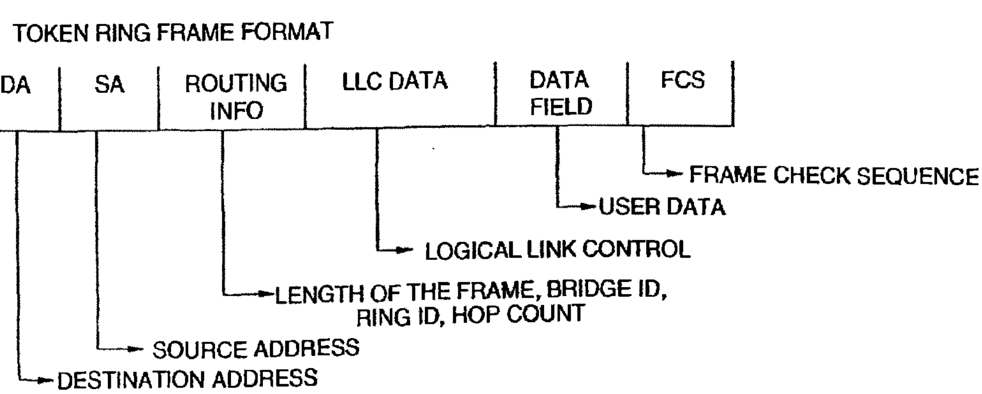


FIG. 4C

DISCOVERY REQUEST

FRAME TYPE IDENTIFIER	TIME STAMP	
1	4	BYTES

FIG. 5A

DISCOVERY RESPONSE

FRAME TYPE IDENTIFIER	INTERCONNECT DEVICE MAC ADDRESS	INTERCONNECT DEVICE DESCRIPTION	TIME STAMP	
1	6	50	4	BYTES

FIG. 5B

SECURITY BREACH DETECTED FRAME

FRAME TYPE IDENTIFIER	INTRUDING MAC ADDRESS	MODULE NUMBER	PORT NUMBER	TIME STAMP	DEVICE FIELD LENGTH	ADDRESSES	
1	6	1	1	4	2	VARIABLE LENGTH	BYTES

FIG. 5C

FILTER SET FRAME

FRAME TYPE IDENTIFIER	INTERCONNECT DEVICE MAC ADDRESS	INTRUDING MAC ADDRESS	MODULE NUMBER	PORT NUMBER	TIME STAMP	
1	6	6	1	1	4	BYTES

FIG. 5D

SECURITY CLEAR CONDITION

FRAME TYPE IDENTIFIER	INTRUDING MAC ADDRESS	
1	6	BYTES

FIG. 5E

INTERCONNECT DEVICE LIST ITEM			
MAC ADDRESS	DEVICE DESCRIPTION	LAST RESPONSE TIME	OUTSTANDING BREACH RESPONSE COUNT

MAC ADDRESS: MAC ADDRESS OF THE INTERCONNECT DEVICE

DEVICE DESCRIPTION: ASCII SELF DESCRIPTION PROVIDED BY THE INTERCONNECT DEVICE

LAST RESPONSE TIME: TIME WHEN LAST RESPONSE RECEIVED FROM INTERCONNECT DEVICE

OUTSTANDING BREACH RESPONSE COUNT: NUMBER OF SECURITY BREACH FRAMES THE INTERCONNECT DEVICE HAS NOT RESPONDED TO

FIG. 6

BREACH LIST ITEM				
MAC ADDRESS	BREACH TIME	BREACH PORT	BREACH MODULE	OUTSTANDING FILTER SET COUNT

MAC ADDRESS: MAC ADDRESS OF THE INTRUDING DEVICE

BREACH TIME: TIME WHEN INTRUSION OCCURRED

BREACH PORT: PORT IN MANAGED HUB WHEN INTRUSION OCCURRED

BREACH MODULE: MODULE IN MANAGED HUB WHEN INTRUSION OCCURRED

OUTSTANDING FILTER SET COUNT: NUMBER OF FILTER SET FRAMES NOT RECEIVED YET

FIG. 7

INTRUSION LIST ITEM			
MAC ADDRESS	BREACH TIME	BREACH PORT	BREACH MODULE

MAC ADDRESS: MAC ADDRESS OF THE INTRUDING DEVICE

BREACH TIME: TIME WHEN INTRUSION OCCURRED

BREACH PORT: PORT IN MANAGED HUB WHEN INTRUSION OCCURRED

BREACH MODULE: MODULE IN MANAGED HUB WHEN INTRUSION OCCURRED

FIG. 8

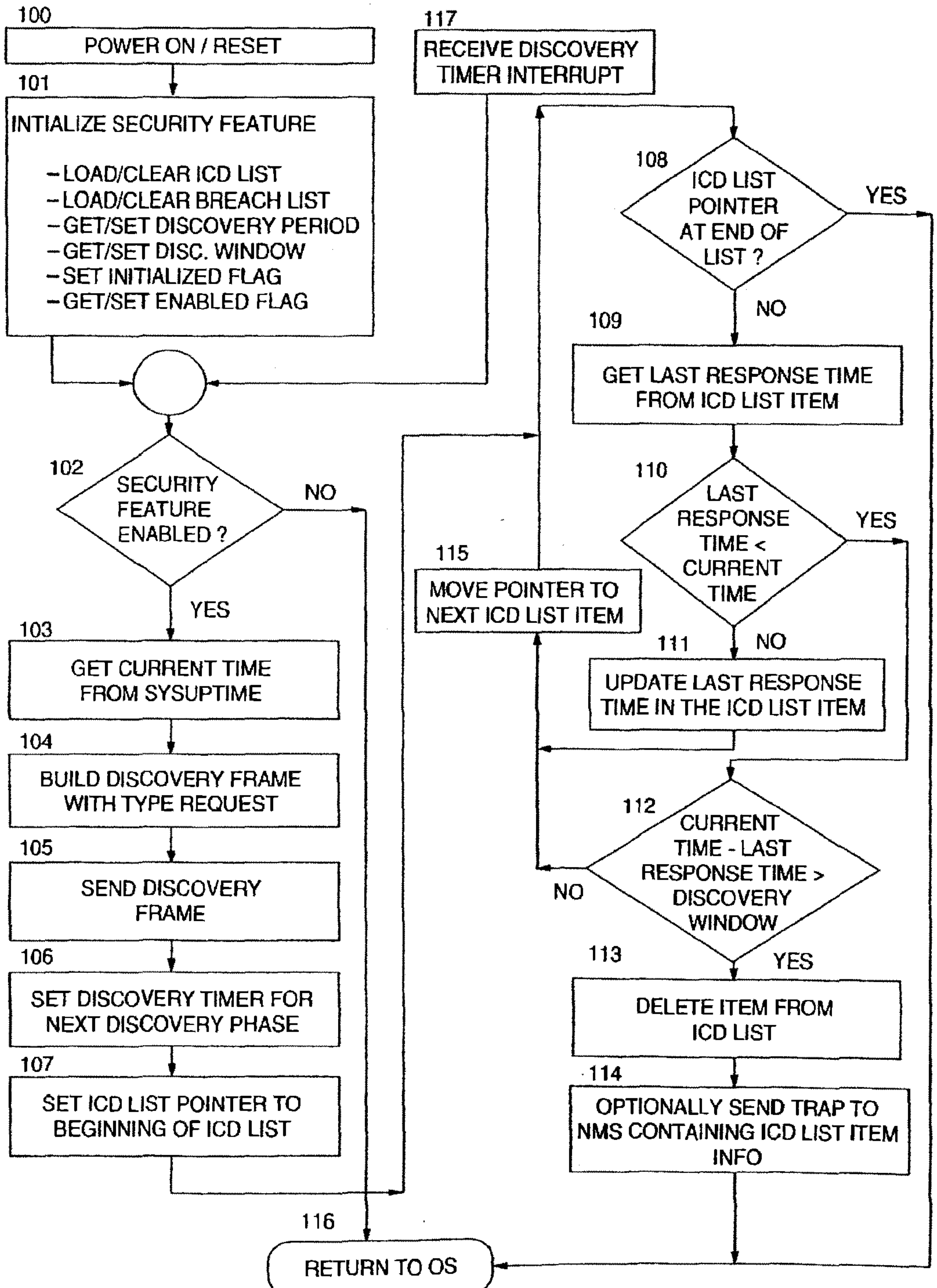

100
POWER ON / RESET
101
INTIALIZE SECURITY FEATURE
–LOAD/CLEAR ICD LIST
–LOAD/CLEAR BREACH LIST
–GET/SET DISCOVERY PERIOD
–GET/SET DISC. WINDOW
–SET INITIALIZED FLAG
–GET/SET ENABLED FLAG
117
RECEIVE DISCOVERY TIMER INTERRUPT
102
SECURITY FEATURE ENABLED ?
NO
YES
103
GET CURRENT TIME FROM SYSUPTIME
104
BUILD DISCOVERY FRAME WITH TYPE REQUEST
105
SEND DISCOVERY FRAME
106
SET DISCOVERY TIMER FOR NEXT DISCOVERY PHASE
107
SET ICD LIST POINTER TO BEGINNING OF ICD LIST
108
ICD LIST POINTER AT END OF LIST ?
YES
NO
109
GET LAST RESPONSE TIME FROM ICD LIST ITEM
110
LAST RESPONSE TIME < CURRENT TIME
YES
NO
115
MOVE POINTER TO NEXT ICD LIST ITEM
111
UPDATE LAST RESPONSE TIME IN THE ICD LIST ITEM
112
CURRENT TIME - LAST RESPONSE TIME > DISCOVERY WINDOW
NO
YES
113
DELETE ITEM FROM ICD LIST
114
OPTIONALLY SEND TRAP TO NMS CONTAINING ICD LIST ITEM INFO
116
RETURN TO OS

FIG. 9

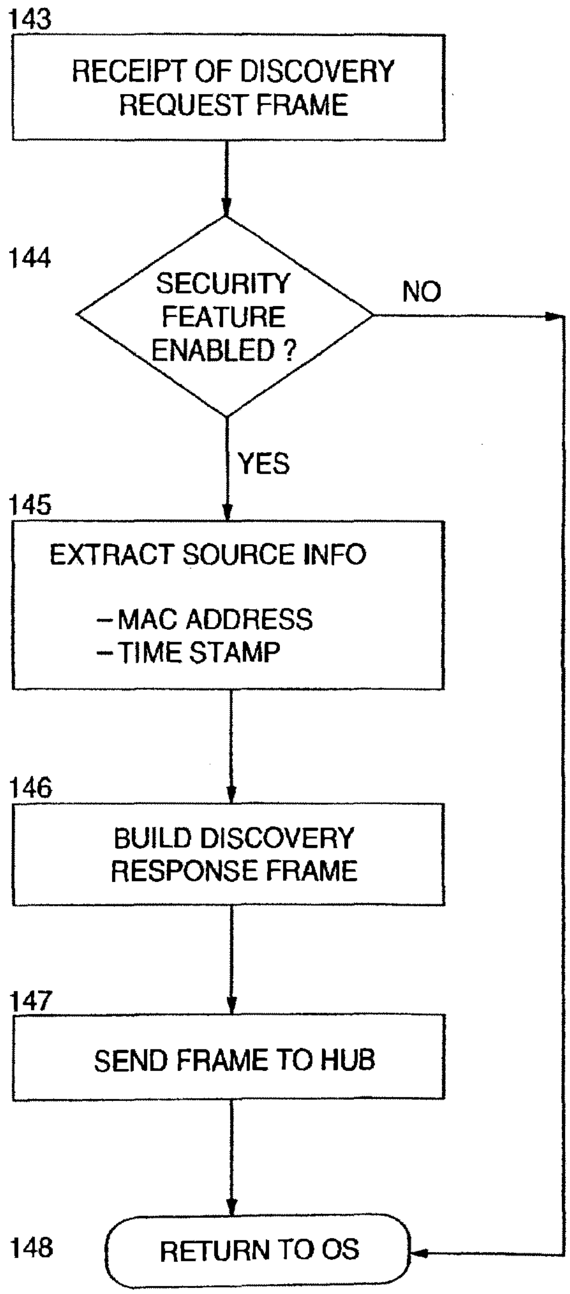

143
RECEIPT OF DISCOVERY REQUEST FRAME
144
SECURITY FEATURE ENABLED ?
NO
YES
145
EXTRACT SOURCE INFO
–MAC ADDRESS
–TIME STAMP
146
BUILD DISCOVERY RESPONSE FRAME
147
SEND FRAME TO HUB
148
RETURN TO OS

FIG. 10

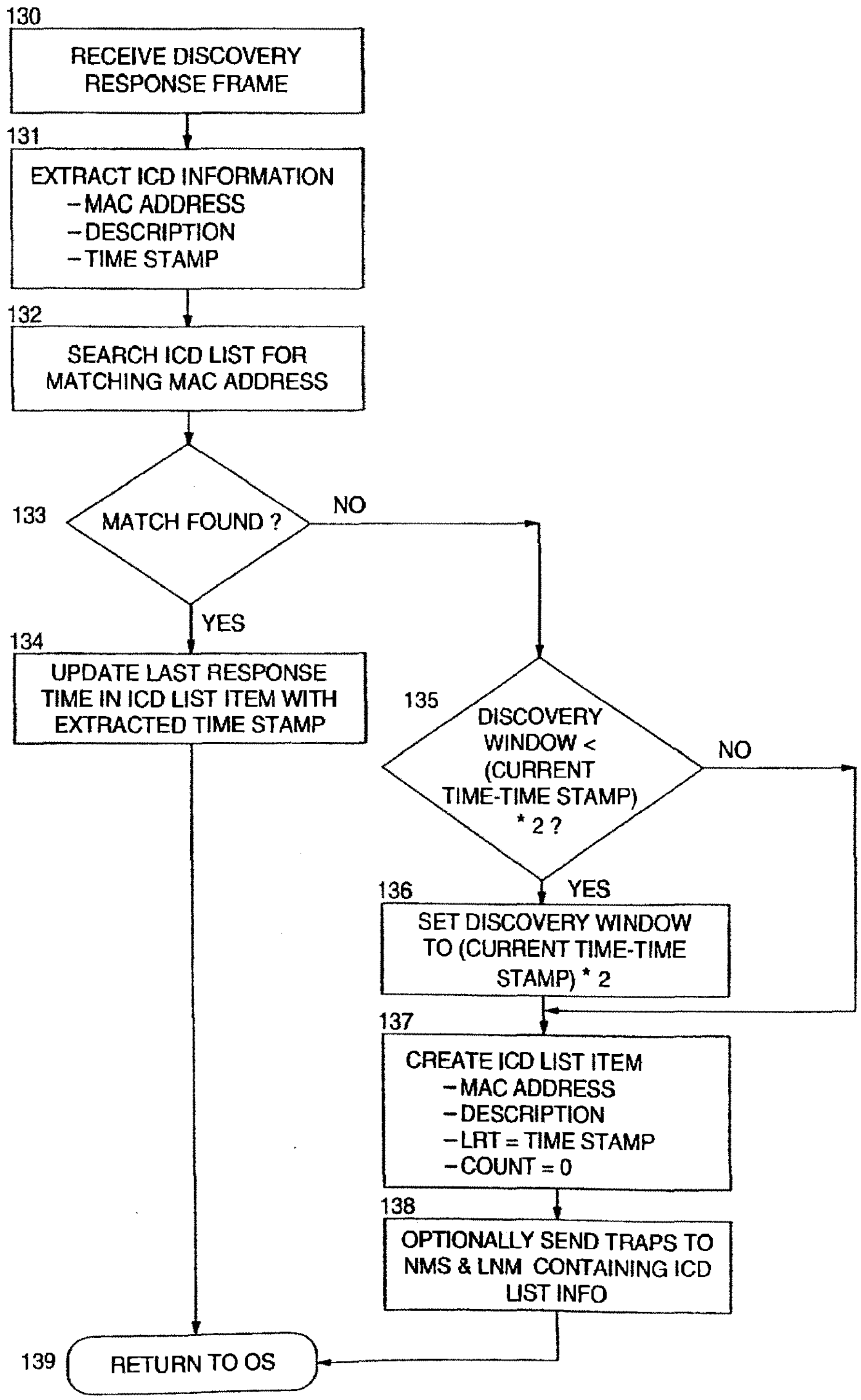

130
RECEIVE DISCOVERY RESPONSE FRAME
131
EXTRACT ICD INFORMATION
–MAC ADDRESS
–DESCRIPTION
–TIME STAMP
132
SEARCH ICD LIST FOR MATCHING MAC ADDRESS
133
MATCH FOUND ?
NO
YES
134
UPDATE LAST RESPONSE TIME IN ICD LIST ITEM WITH EXTRACTED TIME STAMP
135
DISCOVERY WINDOW < (CURRENT TIME-TIME STAMP) * 2 ?
NO
YES
136
SET DISCOVERY WINDOW TO (CURRENT TIME-TIME STAMP) * 2
137
CREATE ICD LIST ITEM
–MAC ADDRESS
–DESCRIPTION
–LRT = TIME STAMP
–COUNT = 0
138
OPTIONALLY SEND TRAPS TO NMS & LNM CONTAINING ICD LIST INFO
139
RETURN TO OS

FIG. 11

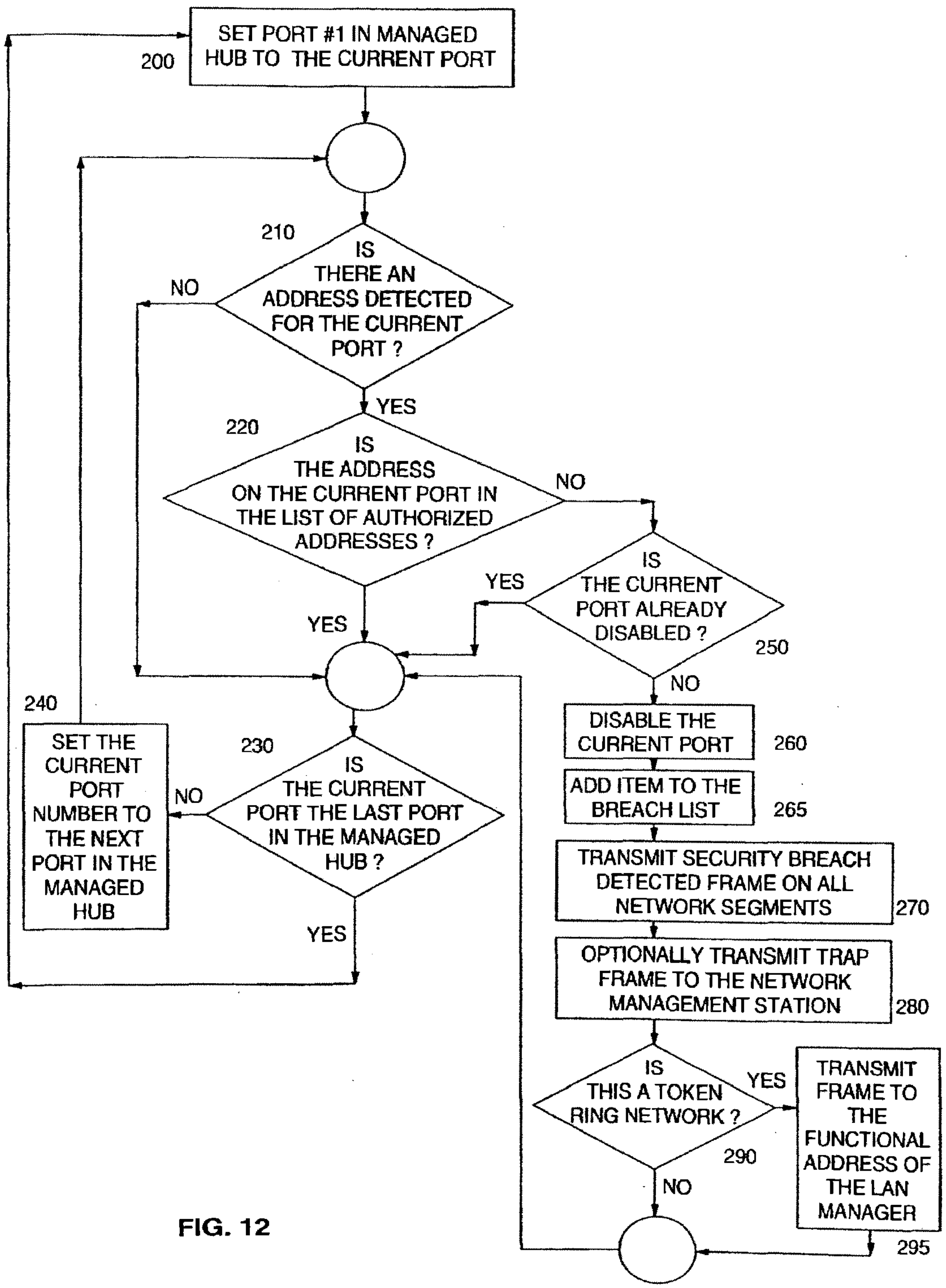

SET PORT #1 IN MANAGED HUB TO THE CURRENT PORT
200
210
IS THERE AN ADDRESS DETECTED FOR THE CURRENT PORT ?
NO
YES
220
IS THE ADDRESS ON THE CURRENT PORT IN THE LIST OF AUTHORIZED ADDRESSES ?
NO
YES
IS THE CURRENT PORT ALREADY DISABLED ?
YES
250
NO
DISABLE THE CURRENT PORT
260
ADD ITEM TO THE BREACH LIST
265
TRANSMIT SECURITY BREACH DETECTED FRAME ON ALL NETWORK SEGMENTS
270
OPTIONALLY TRANSMIT TRAP FRAME TO THE NETWORK MANAGEMENT STATION
280
IS THIS A TOKEN RING NETWORK ?
YES
TRANSMIT FRAME TO THE FUNCTIONAL ADDRESS OF THE LAN MANAGER
290
NO
295
240
SET THE CURRENT PORT NUMBER TO THE NEXT PORT IN THE MANAGED HUB
230
IS THE CURRENT PORT THE LAST PORT IN THE MANAGED HUB ?
NO
YES

FIG. 12

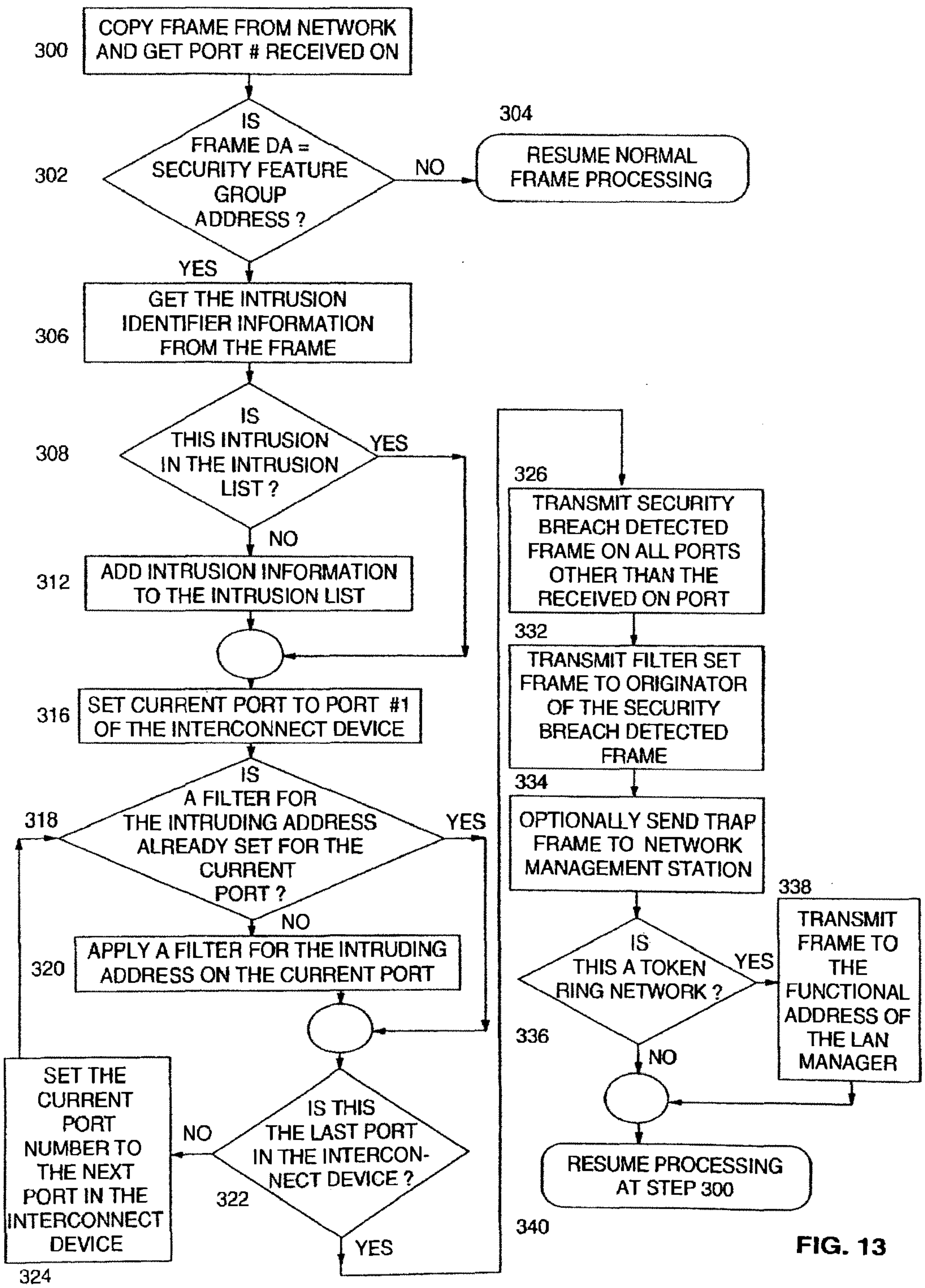

300
COPY FRAME FROM NETWORK AND GET PORT # RECEIVED ON
302
IS FRAME DA = SECURITY FEATURE GROUP ADDRESS ?
NO
304
RESUME NORMAL FRAME PROCESSING
YES
306
GET THE INTRUSION IDENTIFIER INFORMATION FROM THE FRAME
308
IS THIS INTRUSION IN THE INTRUSION LIST ?
YES
NO
312
ADD INTRUSION INFORMATION TO THE INTRUSION LIST
316
SET CURRENT PORT TO PORT #1 OF THE INTERCONNECT DEVICE
318
IS A FILTER FOR THE INTRUDING ADDRESS ALREADY SET FOR THE CURRENT PORT ?
YES
NO
320
APPLY A FILTER FOR THE INTRUDING ADDRESS ON THE CURRENT PORT
IS THIS THE LAST PORT IN THE INTERCON-NECT DEVICE ?
322
NO
YES
SET THE CURRENT PORT NUMBER TO THE NEXT PORT IN THE INTERCONNECT DEVICE
324
326
TRANSMIT SECURITY BREACH DETECTED FRAME ON ALL PORTS OTHER THAN THE RECEIVED ON PORT
332
TRANSMIT FILTER SET FRAME TO ORIGINATOR OF THE SECURITY BREACH DETECTED FRAME
334
OPTIONALLY SEND TRAP FRAME TO NETWORK MANAGEMENT STATION
336
IS THIS A TOKEN RING NETWORK ?
YES
NO
338
TRANSMIT FRAME TO THE FUNCTIONAL ADDRESS OF THE LAN MANAGER
RESUME PROCESSING AT STEP 300
340

FIG. 13

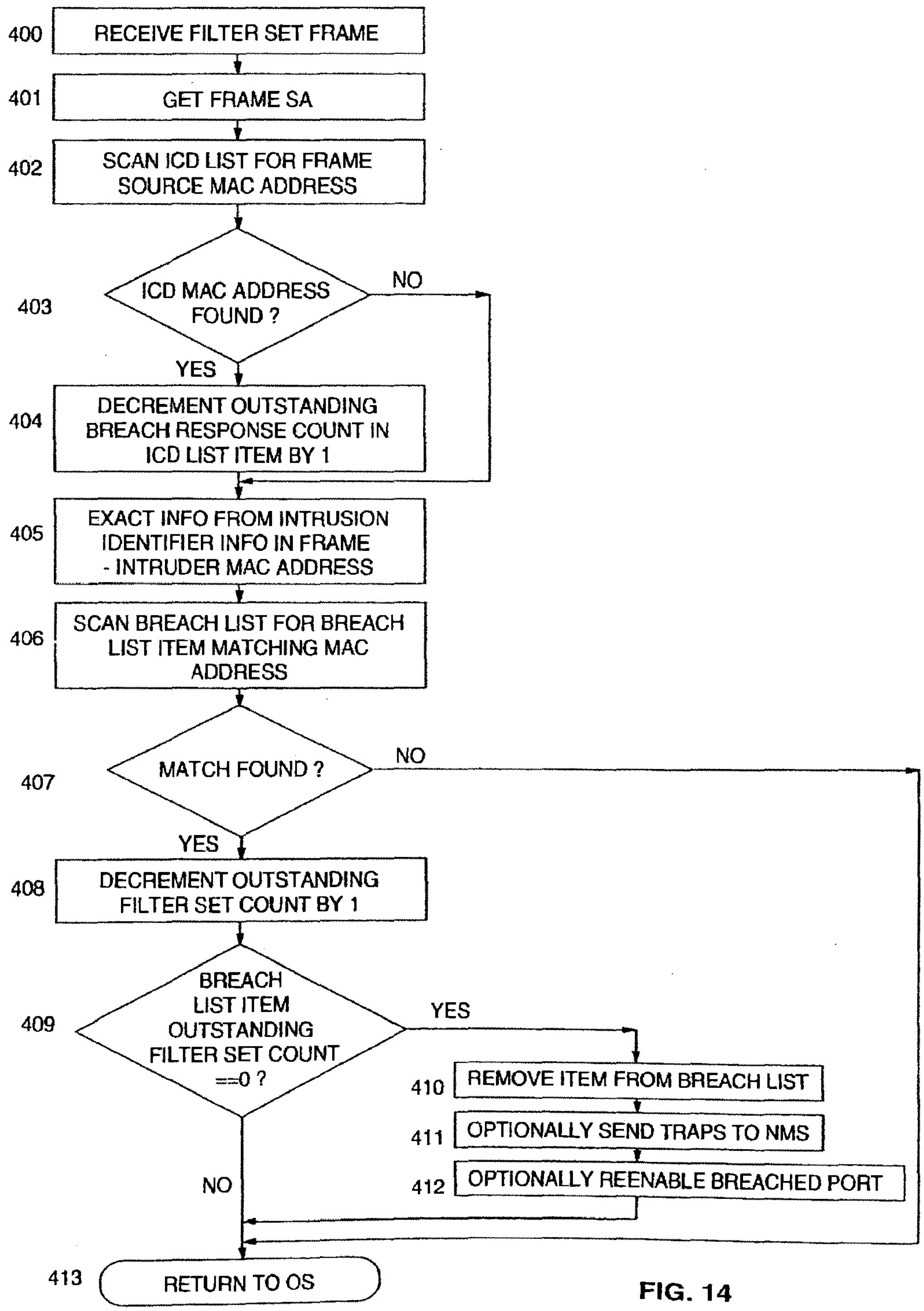

400 RECEIVE FILTER SET FRAME
401 GET FRAME SA
402 SCAN ICD LIST FOR FRAME SOURCE MAC ADDRESS
403 ICD MAC ADDRESS FOUND ?
NO
YES
404 DECREMENT OUTSTANDING BREACH RESPONSE COUNT IN ICD LIST ITEM BY 1
405 EXACT INFO FROM INTRUSION IDENTIFIER INFO IN FRAME - INTRUDER MAC ADDRESS
406 SCAN BREACH LIST FOR BREACH LIST ITEM MATCHING MAC ADDRESS
407 MATCH FOUND ?
NO
YES
408 DECREMENT OUTSTANDING FILTER SET COUNT BY 1
409 BREACH LIST ITEM OUTSTANDING FILTER SET COUNT ==0 ?
YES
NO
410 REMOVE ITEM FROM BREACH LIST
411 OPTIONALLY SEND TRAPS TO NMS
412 OPTIONALLY REENABLE BREACHED PORT
413 RETURN TO OS

FIG. 14

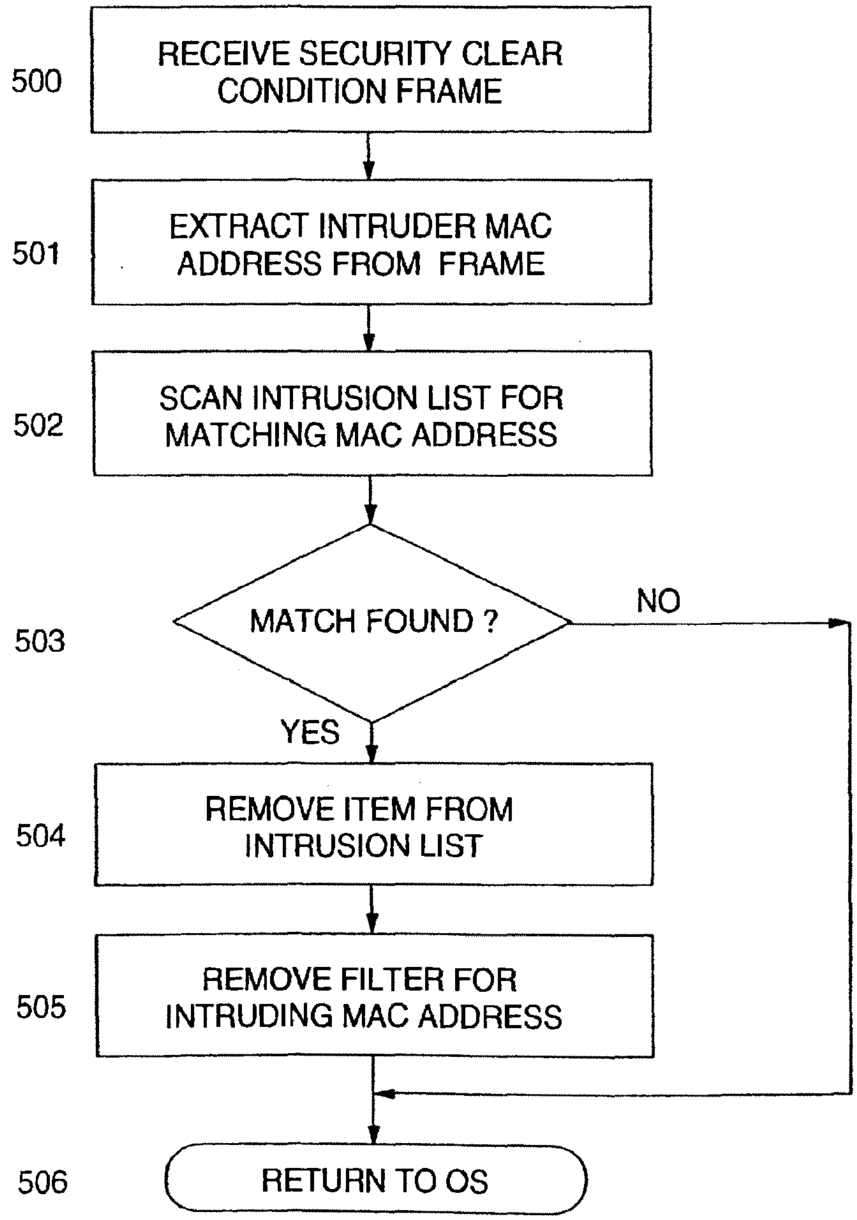

500
RECEIVE SECURITY CLEAR CONDITION FRAME
501
EXTRACT INTRUDER MAC ADDRESS FROM FRAME
502
SCAN INTRUSION LIST FOR MATCHING MAC ADDRESS
503
MATCH FOUND ?
NO
YES
504
REMOVE ITEM FROM INTRUSION LIST
505
REMOVE FILTER FOR INTRUDING MAC ADDRESS
506
RETURN TO OS

FIG. 15

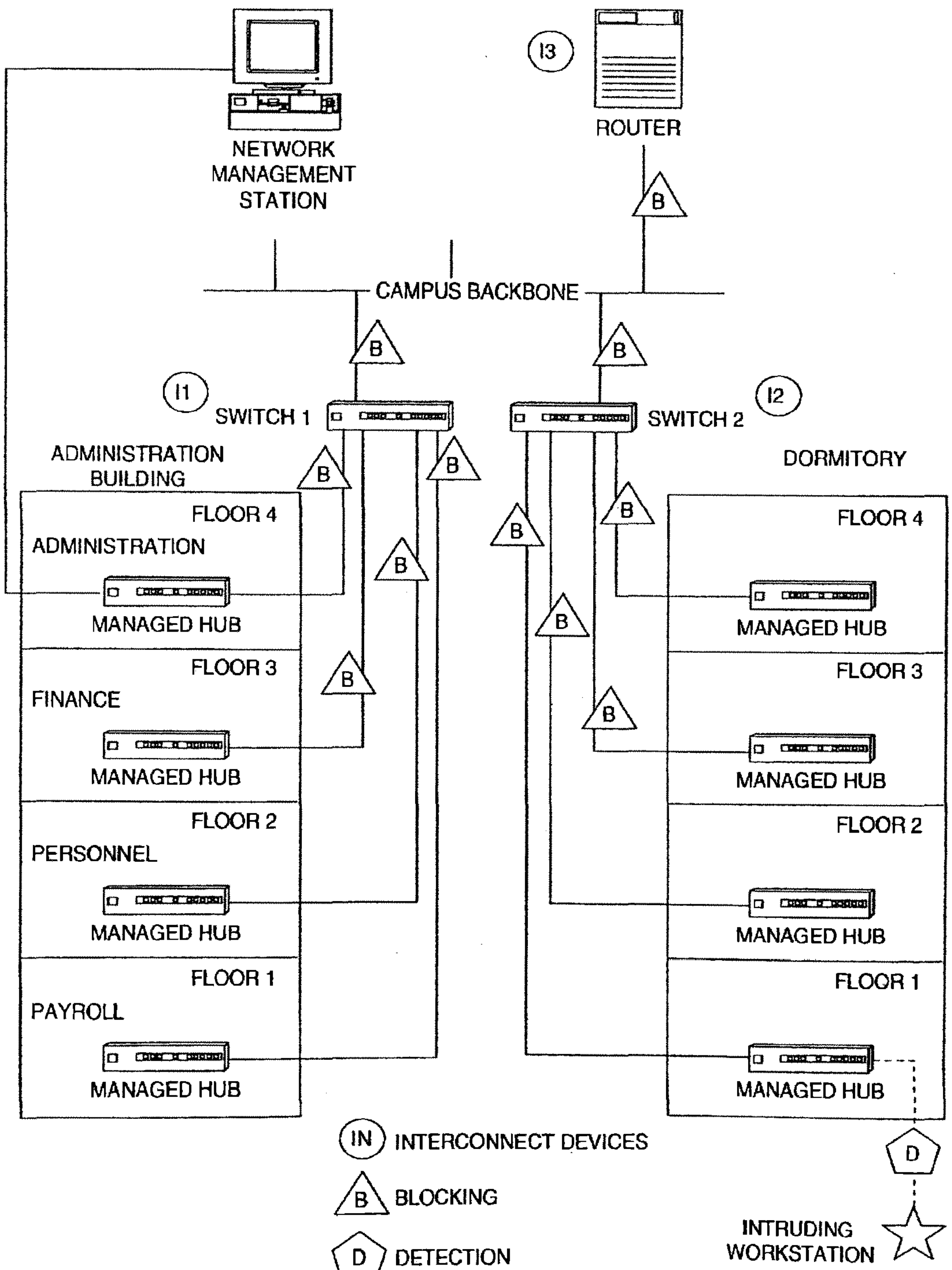
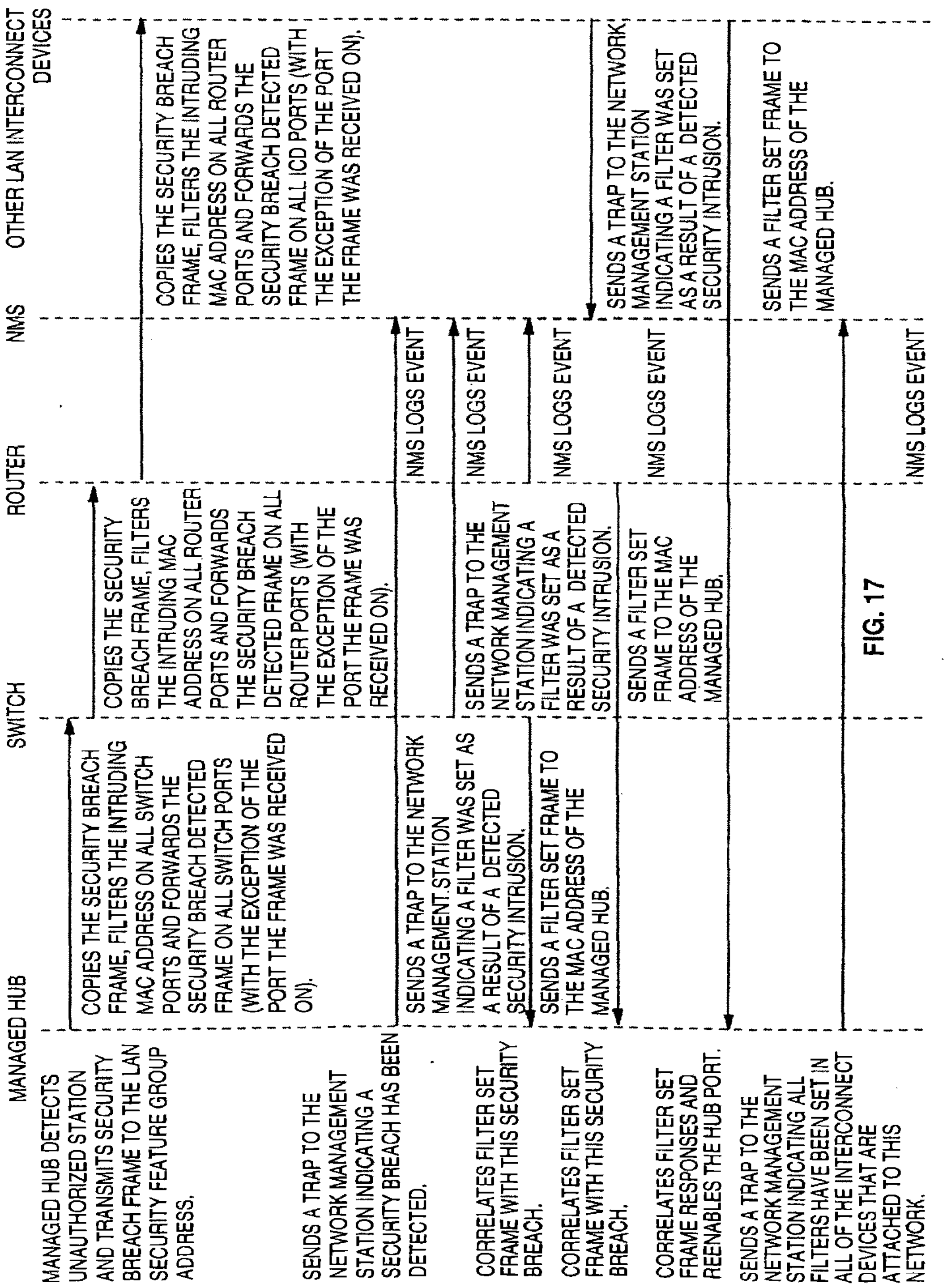

NETWORK
MANAGEMENT
STATION
I3
ROUTER
B
CAMPUS BACKBONE
B
B
I1
SWITCH 1
SWITCH 2
I2
ADMINISTRATION
BUILDING
DORMITORY
B
B
B
B
FLOOR 4
ADMINISTRATION
MANAGED HUB
B
FLOOR 3
FINANCE
MANAGED HUB
FLOOR 2
PERSONNEL
MANAGED HUB
FLOOR 1
PAYROLL
MANAGED HUB
B
B
FLOOR 4
MANAGED HUB
FLOOR 3
MANAGED HUB
FLOOR 2
MANAGED HUB
FLOOR 1
MANAGED HUB
IN
INTERCONNECT DEVICES
B
BLOCKING
D
DETECTION
D
INTRUDING
WORKSTATION

FIG. 16



MANAGED HUB
SWITCH
ROUTER
NMS
OTHER LAN INTERCONNECT DEVICES
MANAGED HUB DETECTS UNAUTHORIZED STATION AND TRANSMITS SECURITY BREACH FRAME TO THE LAN SECURITY FEATURE GROUP ADDRESS.
COPIES THE SECURITY BREACH FRAME, FILTERS THE INTRUDING MAC ADDRESS ON ALL SWITCH PORTS AND FORWARDS THE SECURITY BREACH DETECTED FRAME ON ALL SWITCH PORTS (WITH THE EXCEPTION OF THE PORT THE FRAME WAS RECEIVED ON).
COPIES THE SECURITY BREACH FRAME, FILTERS THE INTRUDING MAC ADDRESS ON ALL ROUTER PORTS AND FORWARDS THE SECURITY BREACH DETECTED FRAME ON ALL ROUTER PORTS (WITH THE EXCEPTION OF THE PORT THE FRAME WAS RECEIVED ON).
COPIES THE SECURITY BREACH FRAME, FILTERS THE INTRUDING MAC ADDRESS ON ALL ROUTER PORTS AND FORWARDS THE SECURITY BREACH DETECTED FRAME ON ALL ICD PORTS (WITH THE EXCEPTION OF THE PORT THE FRAME WAS RECEIVED ON).
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING A SECURITY BREACH HAS BEEN DETECTED.
NMS LOGS EVENT
SENDS A TRAP TO THE NETWORK MANAGEMENT.STATION INDICATING A FILTER WAS SET AS A RESULT OF A DETECTED SECURITY INTRUSION.
NMS LOGS EVENT
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING A FILTER WAS SET AS A RESULT OF A DETECTED SECURITY INTRUSION.
NMS LOGS EVENT
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING A FILTER WAS SET AS A RESULT OF A DETECTED SECURITY INTRUSION.
NMS LOGS EVENT
CORRELATES FILTER SET FRAME WITH THIS SECURITY BREACH.
SENDS A FILTER SET FRAME TO THE MAC ADDRESS OF THE MANAGED HUB.
CORRELATES FILTER SET FRAME WITH THIS SECURITY BREACH.
SENDS A FILTER SET FRAME TO THE MAC ADDRESS OF THE MANAGED HUB.
CORRELATES FILTER SET FRAME RESPONSES AND REENABLES THE HUB PORT.
SENDS A FILTER SET FRAME TO THE MAC ADDRESS OF THE MANAGED HUB.
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING ALL FILTERS HAVE BEEN SET IN ALL OF THE INTERCONNECT DEVICES THAT ARE ATTACHED TO THIS NETWORK.
NMS LOGS EVENT

FIG. 17

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 11, 2008

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:

APPLICATION NUMBER: *09/504,783*
FILING DATE: *February 15, 2000*
PATENT NUMBER: *6,502,135*
ISSUE DATE: *December 31, 2002*

By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office

M. Tarver

M. TARVER
Certifying Officer

PART (4) OF (7) PART(S)

MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS

Reference to Related Application

This application is related to the following application having the same assignee and inventorship and containing common disclosure, and is believed to have an identical effective filing date: "System and Method for Detecting and Preventing Security Intrusions in Campus LAN Networks", Ser. No. 08/780804.

BACKGROUND OF THE INVENTION

This invention relates in general to computer network security systems and in particular to systems and methods for detecting and preventing intrusion into a campus local area network by an unauthorized user.

As local area networks (LANS) continue to proliferate, and the number of personal computers (PCs) connected to LANs continue to grow at a rapid pace, network security becomes an ever increasing problem for network administrators. As the trend of deploying distributed LANs continues, this provides multiple access points to an enterprise's network. Each of these distributed access points, if not controlled, is a potential security risk to the network.

To further illustrate the demand for improved network security, an IDC report on network management, "LAN Management: The Pivotal Role of Intelligent Hubs", published in 1993, highlighted the importance of network security to LAN administrators. When asked the importance of improving management of specific LAN devices, 75% of the respondents stated network security is very important. When further asked about the growing importance of network security over the next three years, many respondents indicated that it would increase in importance.

More recently, a request for proposal from the U.S. Federal Reserve specified a requirement that a LAN hub must detect an unauthorized station at the port level and disable the port within a 10-second period. Although this requirement will stop an intruder, there is an inherent weakness in this solution in that it only isolates the security intrusion to the port of entry. The rest of the campus network is unaware of an attempted break-in. The detection of the unauthorized station and the disabling of the port is the first reaction to a security intrusion, but many significant enhancements can be made to provide a network-wide security mechanism. Where the above solution stops at the hub/port level, this invention provides significant enhancements to solving the problem of network security by presenting a system wide solution to detecting and preventing security intrusions in a campus LAN environment.

In today's environment, network administrators focus their attention on router management, hub management, server management, and switch management, with the goals of ensuring network up time and managing growth (capacity planning). Security is often an afterthought and at best administrators get security as a by-product of employing other device functions. For example, network administrators may set filters at router, switch, or bridge ports for performance improvements and implicitly realize some level of security as a side effect since the filters control the flow of frames to LAN segments.

The problem with using filters is that their primary focus is on performance improvements, by restricting the flow of certain types of network traffic to specified LAN segments. The filters do not indicate how many times the filter has

actually been used and do not indicate a list of the media access control (MAC) addresses that have been filtered. Therefore, filters do not provide an adequate detection mechanism against break-in attempts.

Another security technique that is commonly employed in hubs is intrusion control. There are token ring and Ethernet managed hubs that allow a network administrator to define, by MAC address, one or more authorized users per hub port. If an unauthorized MAC address is detected at the hub port, then the port is automatically disabled. The problem with this solution is that prevention stops at the hub and no further action is taken once the security intrusion has been detected. This solution does not provide a network-centric, system-wide solution. It only provides a piecemeal solution for a particular type of network hardware namely, the token ring and Ethernet managed hubs. The result is a fragmented solution, where security may exist for some work groups that have managed hubs installed, but not for the entire campus network. At best, the security detection/prevention is localized to the hub level and no solution exists for a network-wide solution.

Other attempts to control LAN access have been done with software program products. For example, IBM Corporation's Lan Network Management (LNM) products LNM for OS2 and LNM for AIX both provide functions called access control to token ring LANs. There are several problems with these solutions. One problem with both of these solutions is that it takes a long time to detect that an unauthorized station has inserted into the ring. An intruder could have ample time to compromise the integrity of a LAN segment before LNM could take an appropriate action. Another problem with the LNM products is that once an unauthorized MAC address has been detected, LNM issues a remove ring station MAC frame. Although this MAC frame removes the station from the ring, it does not prevent the station from reinserting into the ring and potentially causing more damage. Because these products do not provide foolproof solutions, and significant security exposure still exists, they do not provide a viable solution to the problem of network security for campus LAN environments.

Thus, there is a need for a mechanism in the managed devices of a computer network that enables a comprehensive solution and that not only provides for detection of security intrusions, but also provides the proactive actions needed to stop the proliferation of security intrusions over the domain of an entire campus network.

SUMMARY OF THE INVENTION

It is, therefore, an object of the invention to provide an apparatus and method in a managed device for detecting and preventing security intrusions in a computer network.

It is another object of the invention to provide an apparatus and method in a managed hub for detecting and preventing security intrusions in a computer network.

Overall, this invention can be described in terms of the following procedures or phases: discovery, detection, prevention, hub enable, and security clear. During each of these phases, a series of frames are transmitted between the interconnect devices on a campus network. These frames are addressed to a group address (multicast address). This well known group address needs to be defined and reserved for the LAN security functions that are described herein. This group address will be referred to as LAN security feature group address throughout the rest of this description.

The campus LAN security feature relies on managed hubs discovering the interconnect devices in the campus LAN segment that support this LAN security feature. The term "LAN interconnect device" is used throughout this description to refer to LAN switches (token ring and Ethernet 10/100 Mbps), LAN bridges and routers. The managed hub maintains a list of authorized MAC addresses for each port in the managed hub. If the managed hub detects an unauthorized station connecting to the LAN, the hub disables the port and then transmits a security breach detected frame to the LAN security feature group address. Each of the LAN interconnect devices on the campus LAN segment copies the LAN security feature group address and performs the following steps: 1) set up filters to filter the intruding MAC address; 2) forward the LAN security feature group address to other segments attached to the LAN interconnect device; and 3) send an acknowledgement back to the managed hub indicating that the intruding address has been filtered at the LAN interconnect device. Once the managed hub receives acknowledgements from all of the interconnect devices in the campus LAN, the port where the security intrusion was detected is re-enabled for use. Another part of the invention provides a network management station with the capability to override any security filter that was set in the above process.

The following is a brief description of each phase in the preferred embodiment of the invention:

1. Discovery

In this phase, the managed hub determines the interconnect devices in the campus network that are capable of supporting the LAN security feature. The managed hub periodically sends a discovery frame to the LAN security feature group address. The managed hub then uses the responses to build and maintain a table of interconnect devices in the network that support the security feature.

2. Detection

In the detection phase, the managed hub compares the MAC addresses on each port against a list of authorized MAC addresses. If an unauthorized MAC address is detected, then the managed hub disables the port and notifies the other interconnect devices in the campus network by transmitting a security breach detected frame to the LAN security feature group address.

3. Prevention

The prevention phase is initiated when a LAN interconnect device receives the security breach detected frame. Once this frame is received, the LAN interconnect device sets up a filter to prevent frames with the intruding MAC address from flowing through this network device. The LAN interconnect device then forwards the security breach detected frame to the other LAN segments attached to the interconnect device. The LAN interconnect device also transmits a filter set frame back to the managed hub.

4. Hub Enable

The hub enable phase takes place when the managed hub has received all acknowledgements from the LAN interconnect devices in the campus network. When the acknowledgements have been received, the managed hub re-enables the port where the security intrusion occurred.

5. Security Clear Condition

In this phase, a network management station can remove a filter from a LAN interconnect device that was previously set in the prevention step.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described with respect to a preferred embodiment thereof which is further illustrated and described in the drawings.

FIG. 1 is a block diagram of a campus network in which the present invention can be implemented.

FIG. 2 is a component block diagram for an SNMP managed device.

FIG. 3 is a component block diagram for a network management station.

FIGS. 4A–4C show general frame formats for Ethernet and token ring frames.

FIGS. 5A–5E show the information contained in the Ethernet and token ring frame data fields to represent the different frame types that are implemented in the preferred embodiment.

FIG. 6 illustrates the structure of the Interconnect Device List (ICD).

FIG. 7 illustrates the structure of the Breach List.

FIG. 8 illustrates the structure of the Intrusion List.

FIG. 9 is a flow chart of the processing that occurs in the managed hub to initiate the discovery phase of the invention.

FIG. 10 is a flow chart of the processing that occurs in the interconnect device during the discovery phase of the invention.

FIG. 11 is a flow chart of the processing that occurs in the managed hub during the discovery phase of the invention in response to the receipt of a discovery response frame.

FIG. 12 is a flow chart of the processing that occurs in the managed hub during the detection phase of the invention.

FIG. 13 is a flow chart of the processing that occurs in an interconnect device during the prevention phase of this invention.

FIG. 14 is a flow chart of the processing that occurs in the managed hub during the hub enable phase of the invention.

FIG. 15 is a flow chart of the processing that occurs in the interconnect devices in response to the receipt of a security clear condition frame.

FIG. 16 is an example of the implementation of the invention in a campus LAN environment.

FIG. 17 is an example of the data flows corresponding to the example implementation in a campus LAN environment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The preferred embodiment of this invention uses the SNMP network management protocol, since SNMP is the most prevalent network management protocol in the industry and is the most widely deployed in campus networks. It should be noted that the concepts in this invention related to network management could also be applied to other network management protocols such as CMIP or SNA.

FIG. 1 illustrates a typical campus network environment in which the present invention can be implemented. As shown in the figure, the campus network 10 contains interconnect devices, such as router 12, router 14, token ring switch 16, bridge 18, managed hubs 20, 22, 24, network management station 26, workstation 28 and file server 30.

The managed hubs and interconnect devices depicted in FIG. 1 are considered SNMP managed devices. The typical component block diagram for an SNMP managed device is illustrated in FIG. 2. A typical managed device is an embedded system that includes a system bus 50, random access memory (RAM) 52, NVRAM 54 to store configuration information, FLASH EPROM 56 to store the operational and boot-up code, a processor or CPU 58 to execute the code instructions, and a media access control (MAC) chip 66 that connects the device to the network 10. FIG. 2 also shows operational code 60, TCP/IP protocol stack 62 and SNMP agent code 64. In most instances, the operational code and the frame processing code execute in FLASH memory 56 or in RAM 52. The code that implements several phases in this invention is included as a part of the operational code (microcode or firmware) of the managed device. The MAC chip 66 copies the frames corresponding to the different phases into RAM 52 and notifies the processor 58, usually via an interrupt, that a frame is ready for processing. The operational code 60 handles the interrupt and processes the frame.

FIG. 3 illustrates the typical component block diagram for a network management station such as that indicated by reference numeral 26 in FIG. 1. The network management station includes a processor 70, with a system bus 90 to which RAM 72, direct access storage device (DASD) 74, other peripherals 76, display monitor 78, keyboard 80, mouse 82 and network interface card 84 are connected.

FIGS. 4A–4C show the general frame formats for Ethernet and token ring frames. The LAN security feature group address is placed in the destination address (DA) field of the discovery request, security breach detected and security clear condition (optionally) frames as discussed more fully below. The data field portion of each frame is used to pass the additional information related to this security feature.

The following describes the information that is included in the data fields of the Ethernet and token ring frame types to represent the different frames that are specific to the preferred embodiment of the invention.

The discovery request frame shown in FIG. 5A is sent to the LAN security feature group address and the data field includes a one byte field which indicates that the frame type (frame type identifier x '01') is a discovery request frame. The time stamp field is the system time value when the discovery request frame is transmitted. It is used to correlate the discovery response frame with the discovery request frame.

The discovery response frame shown in FIG. 5B is sent to the individual MAC address of the managed hub that initiated the request. The data field in this frame includes a one byte field which indicates that the frame type is a discovery response frame (frame type identifier x '02'), and also contains the MAC address of the LAN interconnect device sending the frame, a description of the LAN interconnect device (e.g., IBM 8272 Model 108 Token Ring Switch), and a time stamp that is used to correlate the discovery response frame with the discovery request frame.

The security breach detected frame shown in FIG. 5C is sent to the LAN security feature group address and the data field includes a one byte field which indicates that the frame type is a security breach detected frame (frame type identifier x '03') and contains the MAC address that was detected as the security intruder. Other fields of this frame contain the module number and port number where the security breach was detected and the system time when the security breach was detected. When the time stamp value is used in combination with the intruding MAC address and module and port numbers, it forms an intrusion identifier as will be referred to subsequently. Following the time stamp are device field length indicating the length of the field that follows and address fields. The address field contains the list of addresses that have processed and forwarded the security breach detected frame. It starts with the originating MAC address of the managed hub. Each successive interconnect device that receives the frame, appends its MAC address to the end of this field and updates the device field length before it forwards the frame. It provides an audit trail or path that the security breach detected frame followed throughout the network. A network management station can monitor the progress of the security breach detected frame through information in the trap frames that it receives.

The filter set frame shown in FIG. 5D is sent to the individual MAC address of the managed hub that initiated the security intrusion condition. The data field includes a one byte field which indicates that the frame type is a filt er set frame (frame type identifier x '04') and contains the MAC address of the LAN interconnect device sending the frame. Other fields in this frame are the MAC address of the detected intrusion, the module and port number of the managed hub where the security intrusion was detected, and the time stamp representing the system time when the security breach was detected.

The security clear condition frame shown in FIG. 5E can be sent to the LAN security feature group address or to the individual MAC address of a LAN interconnect device. The data field includes a one byte field which indicates that the frame type is a security clear condition frame (frame type identifier x '05') and contains the intruding MAC address to remove as a filter.

Trap frames are sent to the network management station at various times depending upon the phase of the invention that is being performed. All trap frames have the same basic format with the information in each trap frame varying according to the phase.

In the discovery phase, traps are sent as a result of the managed hub deleting an interconnect device from the list of devices that are in the security domain of interconnect devices. The discovery trap frame contains the trap identifier (x '01'), the MAC address of the interconnect device and device description. This trap indicates that an interconnect device was removed from a managed hub interconnect device list because it did not respond to the managed hub with a discovery response frame within the allotted time period of the discovery window.

Traps sent in the detection phase indicate that the managed hub detected an intrusion on one of the hub ports. Information in this trap frame includes trap identifier (x '02'), the MAC address of the intruding device, the module and port number of the detected intrusion, and the time when the security intrusion was detected.

Traps sent in the prevention phase indicate that the interconnect device has completed the processing of a received security breach detected frame. This trap frame contains the trap identifier (x '03'), the MAC address of the intruding device, the module and port number of the detected intrusion, the time when the security breach was detected and a variable length address field. This last field contains a list of MAC addresses for all the devices that have processed the security breach detected frame. This information provides to the network management station the path that the security breach detected frame followed through the network.

Traps sent in the hub enable phase indicate that the managed hub has reenabled a hub port as a result of receiving filter set frames from all of the interconnect devices in the discovered security domain, i.e., all the discovered interconnect devices. This trap frame contains the trap identifier (x '04'), the MAC address of the intruding device, the module and port number of the detected intrusion, and the time when the security breach was detected.

For token ring networks, the information in the trap frames can be included in frames addressed to the functional address of the LAN manager. The LAN management frame format and defined functional address are specified in the IBM Token Ring Network Architecture (SC30-3374-02) publication.

For managed hubs, the authorized address list (AAL) controls which MAC addresses are allowed to connect to specified ports. Each entry in the AAL consists of two fields: port number and authorized address. The port number identifies a specific port on the hub; the authorized address field specifies the address or addresses that are allowed to connect to the port.

The AAL can be built by the network administrator as part of the configuration of the managed hub. The network administrator identifies the addresses that are allowed to connect to specific ports on the hub. After the initial configuration, the AAL can be updated in several ways. The network management station can add or delete entries in the AAL by sending SNMP management frames. Since most managed hubs provide a Telnet interface into the device to change configuration parameters, a Telnet session could be used to add or delete entries in the AAL. Also, since most managed hubs provide for the attachment of a local console over an RS232 serial port connection which can be used to change configuration parameters, a local console session can be used to add or delete entries in the AAL.

Alternatively, the AAL can be built dynamically through a learning process. Most managed hubs provide a mechanism in the hardware to capture the addresses of the stations that are attached to the ports of a hub. These learned addresses can be provided to the network management station as those stations authorized to access the hub. These learned addresses are then used as the AAL for the managed hub.

The discovery phase is initiated by each managed hub in the campus network. Its purpose is to determine the LAN interconnect devices in the campus LAN that support the LAN security feature. Each managed hub periodically transmits a discovery frame (FIG. 5A) to the LAN security feature group address. The managed hub then uses the information in the response frame (FIG. 5B) to build and maintain a list of all of the devices that support the LAN security feature. This list is referred to as the Interconnect Device List (ICD). The addresses in this list are used in the hub enable phase to correlate the reception of the filter set frame (FIG. 5D) with entries in the list. The managed hubs typically store these ICD lists in management information base (MIB) tables where they can be retrieved, upon request, from a network management station.

The discovery phase can also be used to provide an integrity check on the ICD list of devices supporting the LAN security feature. By periodically transmitting the discovery frame (FIG. 5A) to the LAN security feature group address, checks can then be made to ensure that all of the devices are still in the ICD security list. If any discrepancies are detected, e.g., if a station is removed from the list or added to the list, then an SNMP trap is sent to the network management station. This notification alerts the network administrator that a potential security exposure exists in the campus network. FIG. 6 illustrates the structure of the ICD list along with the information stored in the list for each discovered interconnect device. Other lists that are built and maintained in the detection and prevention phases are the Breach List shown in FIG. 7 and the Intrusion List shown in FIG. 8. Their use will be explained below in the description of the detection and prevention phases.

The detection phase operates at the managed hub level. Each port on the managed hub can be configured to hold one or more MAC addresses of users that are authorized to access the network. The managed hubs can be 10 or 100 Mbps Ethernet or token ring hubs. Current hub chipsets provide the capability to determine the last source MAC address that is seen on a port. When a station attempts to connect to a network, either by inserting into the token ring or by establishing a link state with an Ethernet hub, the last source address seen on the port is compared to the authorized list of MAC addresses that has been defined for this port. If the address is authorized then normal network operations occur. If the address is not authorized, then the managed hub performs the following actions:

1. disables the port;
2. sends an SNMP trap frame to the network management station;
3. sends an alert frame to the functional address of the LAN Manager (token ring); and
4. transmits a security breach detected frame (FIG. 5C) to the LAN security feature group address.

Additional variables in the SNMP trap provide information about the point of intrusion: e.g. the module id (in the case of stackable hubs), the port number, the network number (in cases where hubs have multiple backplanes), and a time stamp (sysUpTime) of when the intrusion was detected. SysUpTime is an SNMP MIB variable that represents the time (units of 0.01s) since the network management portion of the system was last re-initialized.

Some managed hubs support multiple backplanes or networks. In this case, the security breach detected frame is transmitted on all of the active backplanes/networks within the hub.

The well known group address needs to be defined and reserved for LAN security functions. The security breach detected frame (FIG. 5C) containing the MAC address of the station that intruded into the network is sent to the LAN security feature group address.

The prevention phase spans the network. Each interconnect device in the campus network is configured to copy frames addressed to the LAN security feature group address. Upon a security intrusion, the network interconnect devices copy the security breach detected frame (FIG. 5C) and perform the following functions:

1. set filters based on the intruder's MAC address.
2. transmit a security breach detected frame (FIG. 5C) to the LAN security feature group address.
3. send an SNMP trap frame to the network management station.
4. send an alert frame to the functional address of the LAN manager (token ring).
5. transmit filter set frame (FIG. 5D) to the MAC address of the hub that initiated the security breach process.

Setting filters by the network interconnect device prevents intrusion attempts with this MAC address originating elsewhere in the campus network from flowing through this interconnect device. This protects an enterprise's data on this segment of the network from any attacks via the intruder's MAC address.

The interconnect device extracts the intrusion identifier information from the security breach detected frame. If this is the first time the interconnect device has received a security breach detected frame with this intrusion identifier, the interconnect device adds this information to the Intrusion List, then checks to ensure the filter has been set for the intruding MAC address and resets, if required. The interconnect device then transmits the security breach detected frame on all ports except the port on which the security breach detected frame was received.

Sending the trap frame indicates that the filter has been set as a result of receiving the security breach detected frame. Likewise, sending the alert frame indicates that the filter has been set as a result of receiving the security breach detected frame.

The hub enable phase operates at the network level. The hub that initiates the security breach process receives the filter set frames from the interconnect devices in the campus network. The hub then waits to receive responses back from all of the interconnect devices that were determined in the discovery phase to be in the campus network. When all the interconnect devices in the network have responded to the hub with the filter set frame, the hub then re-enables the port for use and then sends a TRAP frame back to the network management station indicating that all filters have been set for the intruding MAC address. The network management station can optionally forward this information to a network management application such as IBM Corporation's NetView/390 product via an alert.

The security clear condition phase of this invention provides the capability for a network administrator to manually override, if necessary, one of the filters that has been set in the prevention phase. The network management station could globally clear, i.e., remove a filter from all LAN interconnect devices by transmitting the security clear condition frame (FIG. 5E) to the LAN security feature group address. The network management station could selectively clear, i.e., remove a filter from a LAN interconnect device by transmitting the security clear condition frame to the MAC address of the specific LAN interconnect device.

FIGS. 9–15 are flow charts that illustrate the processing that occurs in the managed hub and in the interconnect devices during each phase of the invention. The code to implement the discovery phase of this invention runs within the managed hub and interconnect device as event driven threads within the real time OS embedded system. The flows in FIG. 9 depict the processing that occurs in the managed hub to initiate each discovery phase. This task manages the initialization and update of the Interconnect Device List and timing of the next iteration of the discovery phase. The following briefly describes each logic block in the figure.

Step **100**: Entry to this task can be caused by a power on and/or reset. This would be one of many tasks that would run in response to this event.

Step **101**: There are two lists, a period, a window, and two flags that are used by the managed hub in this invention. The ICD (Interconnect Device) List contains information on the devices found during the discovery phase. The Breach List contains information on intrusions recognized by the hub and in the process of being secured. The period is the time between discovery phases. The window is the time between when a discovery phase is initiated and when an Interconnect Device must respond before being assumed inaccessible due to network or device outage. One flag is an indication that initialization has completed. The other flag is an indication that the security feature is enabled. The lists, the period, the window and the enabled flag may be cleared or loaded from persistent memory. The initialized flag is set to True.

Step **102**: Test for whether the security feature is enabled.

Step **103**: Each managed hub maintains a MIB variable that is called SysUpTime. This is used as a time stamp for security feature frames.

Step **104**: The discovery frame is built with the data field containing the type of the frame—Request.

Step **105**: The frame is sent to the LAN security feature group address.

Step **106**: The discovery phase is initiated periodically as an integrity check on the security feature coverage within the network. The period is adjustable to reflect variable path lengths or round-trip-times between a managed hub and interconnect devices. The period can be set via SNMP. The longer t he period, the less the integrity of the network coverage. The shorter the period, the higher the traffic rate required for the security feature.

Step **107**: Set a pointer to the he ad of the list of ICD (Interconnect Device) List items. The pointer may point to an item or nothing if there are not items in the list. (The ICD List is a list of the interconnect devices that responded in a previous discovery phase). This part of the task is to update the Interconnect Device List by updating items as appropriate or deleting them as necessary.

Step **108**: Does the pointer point to an item in the list or does it point beyond the end of the list?

Step **109**: Each ICD List item has a time stamp from the last discovery response frame received from the device.

Step **110**: Is the time for the item in the ICD List later than current time?

Step **111**: If yes, the managed hub has reset or rolled over its SysUpTime since the last response from the ICD. Set the time in the ICD List item to current time.

Step **112**: Is the difference between the current time and the last response time from the item greater than the discovery window?

Step **113**: Assume the device is inaccessible due to network or device outage and purge the item from the ICD List. Also, decrement the outstanding filter set count on all the Breach List items.

Step **114**: If there is a network management station (NMS) that is receiving traps from the managed hub and the traps are enabled, send a trap indicating that the interconnect device is no longer accessible. If there is an LNM for OS/2 station available and traps are enabled, send a trap to the LNM for OS/2 station.

Step **115**: Move the ICD List pointer to the next item or to the end of the list if no more entries exist. This is for stepping through the entire list of ICD items.

Step **116**: End the task and return to the embedded system OS.

Step **117**: Enter this task due to a timer driven interrupt (set in step **106**).

The flows in FIG. **10** depict the processing that occurs in the interconnect devices during each iteration of the discovery phase. This task responds to the receipt of a discovery request frame by sending a discovery response frame. The following briefly describes each logic block in the figure.

Step **143**: The task is initiated by the receipt of a discovery request frame.

Step **144**: A check is made for whether the security feature is enabled. This determines if any additional processing is required.

Step **145**: The source MAC address and time stamp are extracted for building the response.

Step **146**: The discovery response frame is built using the information from the discovery request frame that was just received.

Step **147**: The frame is sent to the originating managed hub.

Step **148**: The task ends, returning control to the embedded OS.

The flows in FIG. **11** depict the processing that occurs in the managed hub in response to the receipt of a discovery response frame. This task maintains the state of this iteration of the discovery phase. The following briefly describes each logic block in the figure.

Step 130: The task is initiated in the managed hub by the receipt of a discovery response frame.

Step 131: The interconnect device information is extracted from the frame.

Step 132: The Interconnect Device List is searched for an item with a MAC address matching the source address of the discovery response frame.

Step 133: Has a match been found?

Step 134: If a match is found, update the last response time in the ICD List item with the time stamp that was extracted from the discovery response frame.

Step 135: If there is no match, assume that the device is not in the list because of either network/device outages or the device has just started utilizing the security feature. It is necessary to determine if the discovery window is still large enough. The round-trip-time is calculated, and multiplied by 2 to derive a potential discovery window. If this is larger than the current discovery window, the discovery window needs to be changed.

Step 136: Change the discovery window.

Step 137: Create a new Interconnect Device List item using the source address from the discovery response frame, the device description from the frame, and the time stamp from the frame. Add it to the list.

Step 138: Optionally send a trap to the network management station(s) and if this is a token ring, to the LAN manager functional address.

Step 139: The task ends, returning control to the embedded OS.

The code to implement the detection phase of this invention runs as a separate task independent from the other tasks in the managed hub. The flows in FIG. 12 depict the processing that occurs during the dispatch of the detection phase task. This task simply checks all the ports in the hub to ensure that the station attached to the port has been authorized to establish a connection on this port. The AAL (Authorized Address List) defines which MAC addresses are allowed to connect to specific ports on the hub. The following briefly describes each logic block in the figure.

Step 200: This is the entry point for the detection phase task. Processing starts at port number 1 in the hub and continues until all of the ports in the hub have been processed.

Step 210: This step checks if a station is attached to the port in the hub. If a station is attached, then an address exists for the port. If an address is detected for the port (i.e., a station is attached to the port), then processing continues with step 220. if there is no address detected for this port (i.e., no station is attached), then processing continues with step 230.

Step 220: A check is made here to ensure that the address that has been detected on this port is in the list of authorized addresses. If the address detected on the port is authorized, then continue processing at step 230. If the address detected on the port is not in the authorized list, then processing continues at step 250.

Step 230: A check is made here to see if all of the ports in the hub have been processed. If all of the ports have been processed, then processing resumes at step 200 with the processing of port number 1. if this was not the last port and there are more ports to process, then processing continues at step 240.

Step 240: In this step, the next port in the hub is set up to be processed. Processing then continues at step 210.

Step 250: In this step a check is made to see if the port is already disabled. If the port is already disabled, then the port/network is already secure from intruders on this port. if the port is already disabled, then processing continues at step 230. If the port is enabled, processing then continues at step 260.

Step 260: In this step, the port is disabled. Processing then continues at step 265.

Step 265: In this step, an entry is added to the Breach List containing the following: MAC address that was detected as the intruder, the module and port number where the intrusion was detected, the time (sysUpTime) when the security breach was detected, and the outstanding filter set count which is set to the number of entries in the ICD list. Processing then continues at step 270.

Step 270: In this step, the security breach detected frame is transmitted on all network segments of the hub. The info field of the security breach detected frame includes the following: MAC Address of the intruder, module number, port number, time stamp (sysUpTime), the device field length initialized to 6 (bytes), the 6 byte MAC address of the managed hub. Processing then continues at step 280.

Step 280: In this step, a trap frame is optionally sent to the network management station. The trap frame includes the following information:

(a) trap identifier x '02';

This indicates that the managed hub detected in intrusion on one of the hub ports.

(b) MAC address of the intruding device;

(c) module number of the detected intrusion;

(d) port number of the detected intrusion;

(e) time when the security breach was detected;

Processing then continues at step 290.

Step 290: In this step, a check is made to see if this invention has been implemented in a token ring network. The token ring architecture defines a special functional address that is used by LAN management stations. Functional addresses are only used in token ring environments. If the invention is implemented in a token ring network, processing then continues at step 295. If the invention is implemented in a non-token ring network, processing then continues at step 230.

Step 295: in this step, a frame is sent to the functional address of the LAN manager with the information from step 280. Processing then continues at step 230.

FIG. 13 depicts the flows for the prevention phase of the invention. The prevention phase is implemented in the interconnect devices of the network. The following briefly describe each logic block in the figure.

Step 300: The processing is initiated when the interconnect device receives a frame from the network. The interconnect device copies the frame and saves the port number that the frame was received on. Processing then continues at step 302.

Step 302: In this step, the frame that wa s copied in step 300 is interrogated and a check is made to determine if the destination address of the frame is equal to the LAN security feature group address. if the received frame is addressed to the LAN security feature group address, then processing continues at step 306. Otherwise, the frame is of some other type and the processing continues with step 304.

Step 304: This step is encountered for all frame types other than the LAN security feature. The normal frame processing code of the interconnect device runs here.

Step 306: In this step, the intrusion identifier information is copied from the frame. The intrusion identifier consists of the following information:

(a) MAC address of the intruder;

(b) module number;

(c) port number;

(d) time stamp;

Processing then continues at step **308**.

Step **308**: In this step, a check is made to determine if the intrusion identifier is already in the Intrusion List of this interconnect device. If yes, processing then continues at step **316**. If no, processing then continues at step **312**.

Step **312**: In this step, the intrusion identifier information is added to the Intrusion List. Processing then continues at step **316**.

Step **316**: In this step, the current port of the interconnect device is set to port number 1. Processing then continues at step **318**.

Step **318**: In this step, a check is made to determine if the intruding MAC address is already filtered on the current port. If yes, processing then continues at step **322**. If no, processing then continues at step **320**.

Step **320**: In this step, a filter is set for the intruding MAC address on the current port. Processing then continues at step **322**.

Step **322**: In this step a check is made to determine if the filter processing has been applied to all of the ports in the interconnect device. If all of the ports have been processed, processing then continues at step **326**. If there are more ports to process, processing then continues at step **324**.

Step **324**: In this step, the current port is set to the next port in the interconnect device. Processing then continues at step **318**.

Step **326**: In this step, the security breach detected frame is propagated throughout the network. The interconnect device transmits the security breach detected frame on all ports other than the port the original frame was received on. (Reference step **300** where it is determined which port the frame was received on). Before transmitting the security breach detected frame, the ICD appends its MAC address to the addresses field of the frame and increments the device field length field of the frame by 6. This provides the audit trail or the path information for the security breach detected frame. Processing then continues at step **332**.

Step **332**: In this step, the interconnect device transmits the filter set frame to the originator of the security breach detected frame. The originator is determined by extracting the source address from the frame that was copied in step **306**. Processing then continues at step **334**.

Step **334**: In this step, a trap frame is sent to the network management station. The trap frame includes the following information:

(a) trap identifier x '03';

This indicates that the interconnect device has completed the processing of a received security breach detected frame.

(b) MAC address of the intruding device;

(c) module number of the detected intrusion;

(d) port number of the detected intrusion;

(e) time when the security breach was detected;

(f) addresses field;

This is a variable length field that contains a list of all of the devices that have processed the security breach detected frame. This information provides to the network management station the path that the security breach detected frame followed throughout the network.

Processing then continues at step **336**.

Step **336**: In this step, a check is made to see if this invention has been implemented in a token ring network. The token ring architecture defines a special functional address that is used for LAN management stations. Functional addresses are only used in token ring environments. If the invention is implemented in a token ring network, processing then continues at step **338**. If the invention is implemented in a non-token ring network, processing then continues at step **340**.

Step **338**: In this step, a frame containing the same information in the trap frame in step **334** is sent to the functional address of the LAN manager. Processing then continues at step **340**.

Step **340**: In this step, processing resumes again at step **300**.

The code to implement the hub enable phase of this invention runs within the managed hub as event driven threads within the real time OS embedded system. The flows in FIG. **14** depict the processing that occurs in the managed hub in response to receipt of each filter set frame. The task maintains the necessary lists of interconnect devices and breaches to complete the hub enable phase for each breach. The following briefly describes each logic block in the figure.

Step **400**: The task is initiated in the managed hub by the receipt of a filter set frame.

Step **401**: Get the source address of the frame for finding the associated ICD List item.

Step **402**: The Interconnect Device List is scanned for an item with the same MAC address as the source address of the frame.

Step **403**: Was a match found? If not, assume that the interconnect device is no longer accessible.

Step **404**: If a match is found, decrement the outstanding breach response count in ICD List item by 1. This provides an up-to-date count of outstanding responses for each ICD.

Step **405**: Extract intrusion identifier information from the frame.

Step **406**: Scan the Breach List for an item with a matching intrusion identifier.

Step **407**: Match found?

Step **408**: If a match is found, decrement the outstanding filter set count by 1 in the matching Breach List item.

Step **409**: Have all interconnect devices responded? Are all filters set?

Step **410**: Since the intruder is now being filtered and has been removed from the network, remove the Breach List item.

Step **411**: If there is a listening network management station(s), send a trap. If this is a token ring, send an alert to the LAN manager functional address.

Step **412**: Optionally reenable the port. This is a policy decision. It may also reflect the likelihood of the intruder still attempting to intrude via this same port.

Step **413**: End the task and return control to the embedded OS.

The code to implement the security clear condition phase of this invention runs within the interconnect devices as event driven threads within the real time OS embedded system. The flows in FIG. **15** define the processing that occurs in the interconnect devices in response to receipt of each security clear condition frame. The task updates the Intruder List of breaches and completes the security clear condition phase for each breach. The following briefly describes each logic block in the figure.

Step **500**: The task is initiated in the interconnect device by the receipt of a security clear condition frame from a network management station.

Step **501**: Extract the intruder MAC address from the security clear condition frame.

Step **502**: Search the Intrusion List for a matching MAC address.

Step 503: Is there a match?

Step 504: If there is a match, remove the item from the Intrusion List.

Step 505: Remove filter for the intruding MAC address.

Step 506: End the task and return control to the embedded OS.

Two examples are given below to illustrate the actions that are performed by the managed hub and interconnect devices in an implementation of this invention in an operational campus environment. Referring again to FIG. 1, there is depicted a workstation 28, attached to an Ethernet hub 24, that is attempting to gain unauthorized access to a file server 30 that is located on a token ring segment. The security intrusion is detected by the managed Ethernet hub 24, since the MAC address of the workstation 28 is not authorized for this port in the hub. The managed hub 24 then disables the port and transmits the security breach detected frame to the LAN interconnect device 14 on this segment, which, in turn, forwards the security breach detected frame to LAN interconnect devices 12, 16 that are attached to subnet 3 and subnet 4, respectively. LAN interconnect device 12, in turn, forwards the security breach detected frame to LAN interconnect device 18. The LAN interconnect devices 12, 14, 16, 18 set filters on all ports in the device to prevent frames with the intruding MAC address from flowing through the interconnect device.

More specifically, the managed hub 24 disables the port and transmits the security breach detected frame to router 14. The managed hub 24 also sends a trap frame to the management station 26. Router 14 applies the intruder's MAC address as a filter on all of its ports and forwards the security breach detected frame on all of its ports, except the port the security breach detected frame was received on. Router 14 then sends a trap to the network management station 26 and sends a filter set frame back to the managed hub 24. Router 12 and the token ring switch 16 also receive the security breach detected frame and perform the same processing operations as defined above for router 14. The bridge 18 receives the security breach detected frame and performs the same processing operations as done by router 14. The managed hub 24 now correlates all of the received filter set frames with the interconnect devices 12, 14, 16, 18 that were discovered via the discovery request/response frames and reenables the port. The managed hub 24 then sends a trap to the management station 26 to indicate that the intruder's port has been reenabled.

As a practical example of the implementation of this invention in a campus LAN environment, FIG. 16 depicts a university setting in which there is a managed hub on each floor of the buildings in a campus network. The network infrastructure consists of a pair of Ethernet switches attached to a campus backbone. Each Ethernet switch is also attached to a plurality of Ethernet managed hubs (one on each floor in each building). The figure shows a student dormitory that is attached to the same network that runs the university administration applications. There are obvious security concerns about students accessing the proprietary administrative information (i.e., grades, transcripts, payroll, accounts receivable/payable, etc.).

An intruder trying to access the network via one of the managed hub ports in the dormitory is stopped at the port of entry to the network and further access to the campus network is prevented by having the intruder's MAC address filtered on all LAN interconnect devices. The symbols containing a "B" in FIG. 16 indicate the points in the campus network where frames with the intruding MAC address are blocked from access to LAN segments by the setting of filters. The data flows corresponding to the example are shown in FIG. 17 and are self-explanatory.

For simplicity, this invention has used the term managed hub to refer to traditional token ring and Ethernet port concentration devices (e.g., IBM 8238, IBM 8224, IBM 8225, IBM 8250, IBM 8260). In reality, the functions of the managed hub can be extended to LAN switches (both token ring and Ethernet) where dedicated stations could be attached directly to the switch port. LAN switches would have to add the functionality of authorizing a set of MAC addresses that could attach to a switch port and detecting any unauthorized accesses to the switch port.

To describe the key aspects of this LAN security invention, it was easiest to illustrate with an implementation using managed hubs. In reality, many large enterprises use a combination of both managed hubs and unmanaged hubs throughout their networks. This invention is readily extendible and the security detection mechanism can easily be integrated into the function of a LAN bridge. The bridge would keep the list of authorized addresses for a given LAN segment where access to the LAN is via low cost unmanaged concentrators. The bridge would then detect any new addresses on the LAN segment and compare the addresses against the authorized list. If an unauthorized address was detected, the bridge would then set up filters for the intruding MAC address, and transmit the security breach detected frame to the other interconnect devices attached to the campus network. In this case, the intruder would be isolated to the LAN segment where the intrusion was first detected. This example shows that the composite function of the managed hub could be integrated into a LAN bridge and the bridge could control the security access for a large segment consisting of unmanaged concentrators.

Another special use of this invention involves the tasks of a network administrator. A key day-to-day task for most network administrators falls into the category of moves, adds, and changes to network configuration. In this invention, the network management station has complete awareness of all of the authorized users throughout the campus network. In the event that a security breach is detected, in the special case where an authorized user is trying to gain access through an unauthorized port, the network management station could detect this situation and automatically take the appropriate actions (i.e., remove filters from the interconnect devices since this is an authorized user). This type of action would assist administrators that work in dynamic environments where there are frequent moves, adds and changes.

The preferred embodiment of the invention has relied upon the detection of unauthorized MAC addresses by the managed hub. It can easily be modified to apply to the network layer (layer 3) or higher layers, in the Open System Interconnection (OSI) protocol stack and work with such well known network protocols as TCP/IP, IPX, HTTP, AppleTalk, DECnet and NETBIOS among others.

Currently, many LAN switches have custom application specific integrated circuits (ASICs) that are designed to detect or recognize frame patterns in hardware. These LAN switches use this frame type recognition capability primarily for frame forwarding based on the IP address and for placing switch ports in a virtual LAN (VLAN). In order to provide security protection at the network layer, it will be clear to one skilled in the art that the authorized address list (AAL) described herein can be extended to include IP addresses. The so-modified AAL, coupled with the LAN switch capability to detect IP addresses in a frame will enable implementation of the detection and prevention phases to support

IP addresses. In the detection phase, the ASIC-based LAN switch can be used to obtain the IP address that is connected to a port. The detected IP address would then be compared to the authorized IP addresses in the AAL. If an unauthorized IP address is detected, the invention works as previously described with the disabling of the port and the transmission of the security breach detected frame. In the prevention phase, the interconnect devices are notified of intruding IP addresses and then apply filters for the intruding IP address.

The present invention can also be modified to operate at the application layer (layer 7) of the OSI protocol stack. Currently, several commercially available LAN switches, such as the model 8273 and model 8274 LAN switches available from IBM Corporation, provide a capability for a user-defined policy for creating a VLAN. This user-defined policy enables one to specify an offset into a frame and a value (pattern) to be used to identify the frame. Once the user-defined policy has been defined, the switch ASIC detects all frames matching the specified pattern and places them into a specific VLAN. Since the custom ASIC recognizes the user-defined pattern, it can be programmed to recognize portions of a frame that identify a specific application. This application pattern can then be used as the detection criteria in the invention and thus provide application layer security.

The present invention can be modified further to provide additional security by encryption of the data fields in the frames that are used to implement the inventive concepts described above. One of the most widely known and recognized encryption algorithms is the Data Encryption Standard (DES). The implementation of DES or other encryption algorithm to encrypt the data fields of frames described in this invention can ensure the privacy and integrity of the communication between managed hubs, interconnect devices and network management stations. Security protocols such as Secure Sockets Layer (SSL) utilizing public key encryption techniques are becoming standardized and can be used to further enhance the invention described herein.

While the invention has been particularly shown and described with reference to the particular embodiments thereof, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.

Having thus described our invention, what we claim and desire to secure as Letters Patent is as follows:

1. A method for providing security against intrusion in a managed device of a computer network having at least one interconnect device, said method comprising the steps of:

- discovering each of said interconnect devices that is enabled to provide network security;
- detecting an unauthorized address on a first port of said managed device and disabling said first port;
- notifying each of said security-enabled interconnect devices that the unauthorized address has been detected on said first port; and
- reenabling said first port after each of said security-enabled interconnect devices has notified said managed device that a filter has been set to prevent frames with the unauthorized address from flowing through said each security-enabled interconnect device.

2. The method for providing security against intrusion of claim 1 wherein said managed device is a managed hub.

3. The method for providing security against intrusion of claim 1 wherein said managed device is a switch.

4. The method for providing security against intrusion of claim 1 wherein said computer network includes a local area network.

5. The method for providing security against intrusion of claim 1 further comprising the steps of building and maintaining an authorized address list of addresses that are allowed to connect to each port in said managed device.

6. The method for providing security against intrusion of claim 5 wherein each entry in said authorized address list includes a port number and an authorized address.

7. The method for providing security against intrusion of claim 1 wherein said discovering step includes the steps of:

- transmitting a discovery request frame, said discovery request frame having a security feature group address;
- receiving a discovery response frame from each of said security-enabled interconnect devices;
- building and maintaining an interconnect device list of said security-enabled interconnect devices that transmitted said discovery response frame back to said managed device.

8. The method for providing security against intrusion of claim 7 wherein each entry in said interconnect device list includes an address of the security-enabled interconnect device that sent the discovery response frame and a time stamp extracted from said discovery response frame.

9. The method for providing security against intrusion of claim 6 wherein said detecting step includes the steps of:

- comparing, for each port, a source address of a station attempting to connect to said port with the authorized address list of addresses for said port and determining whether said source address is on said authorized address list.

10. The method for providing security against intrusion of claim 7 wherein following said disabling step said method further includes:

- sending a trap frame to a network management station indicating that an intrusion has been detected on said first port; and
- transmitting a security breach detected frame having said security feature group address to said security-enabled interconnect devices that have entries in said interconnect device list.

11. The method for providing security against intrusion of claim 10 wherein said security breach detected frame includes a source address of an unauthorized station, the port number at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

12. The method for providing security against intrusion of claim 11 wherein each of said security-enabled interconnect devices transmits a filter set frame to said managed device that includes the address of said each security-enabled interconnect device sending said filter set frame, the source address of said unauthorized station, the port number at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

13. The method for providing security against intrusion of claim 1 wherein following said reenabling step said managed device sends a trap frame to a network management station indicating that said filtering step has been completed.

14. An apparatus for providing security against intrusion in a managed device of a computer network having at least one interconnect device, said apparatus comprising:

- means for discovering each of said interconnect devices that is enabled to provide network security;
- means for detecting an unauthorized address on a first port of said managed device and means for disabling said first port;
- means for notifying each of said security-enabled interconnect devices that the unauthorized address has been detected on said first port; and

means for reenabling said first port after each of said security-enabled interconnect devices has notified said managed device that a filter has been set to prevent frames having the unauthorized address from flowing through said each security-enabled interconnect device.

15. The apparatus for providing security against intrusion of claim 14 wherein said managed device is a managed hub.

16. The apparatus for providing security against intrusion of claim 14 wherein said managed device is a switch.

17. The apparatus for providing security against intrusion of claim 14 further comprising means for building and maintaining an authorized address list of addresses that are allowed to connect to each port in said managed device.

18. The apparatus for providing security against intrusion of claim 17 wherein each entry in said authorized address list includes a port number and an authorized address.

19. The apparatus for providing security against intrusion of claim 14 wherein said means for discovering includes:

means for transmitting a discovery request frame, said discovery request frame having a security feature group address;

means for receiving a discovery response frame from each of said security-enabled interconnect devices;

means for building and maintaining an interconnect device list of said security-enabled interconnect devices that transmitted said discovery response frame back to said managed device.

20. The apparatus for providing security against intrusion of claim 19 wherein each entry in said interconnect device list includes an address of the security-enabled interconnect device that sent the discovery response frame and a time stamp extracted from said discovery response frame.

21. The apparatus for providing security against intrusion of claim 18 wherein said means for detecting includes:

means for comparing, for each port, a source address of a station attempting to connect to said port with the authorized address list of addresses for said port and means for determining whether said source address is on said authorized address list.

22. The apparatus for providing security against intrusion of claim 19 further including:

means for sending a trap frame to a network management station indicating that an intrusion has been detected on said first port; and

means for transmitting a security breach detected frame having said security feature group address to said security-enabled interconnect devices that have entries in said interconnect device list.

23. The apparatus for providing security against intrusion of claim 22 wherein said security breach detected frame includes a source address of an unauthorized station, the port number at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

24. The apparatus for providing security against intrusion of claim 23 wherein each of said security-enabled interconnect devices transmits a filter set frame to said managed device that includes the address of said each security-enabled interconnect device sending said filter set frame, the source address of said unauthorized station, the port number at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

25. The apparatus for providing security against intrusion of claim 14 wherein said managed device further comprises means for sending a trap frame to a network management station indicating that said filter has been set at each of said security-enabled interconnect devices.

26. A method for providing security against intrusion in a managed hub of a computer network having at least one interconnect device, said method comprising the steps of:

building and maintaining an authorized address list of addresses that are allowed to connect to each port;

discovering each interconnect device that is enabled to provide network security;

detecting an unauthorized address on a first port and disabling said first port;

notifying each security-enabled interconnect device that the unauthorized address has been detected on said first port; and

reenabling said first port after each security-enabled interconnect device has notified said managed hub that a filter has been set to prevent frames with the unauthorized address from flowing through each security-enabled interconnect device.

27. The method for providing security against intrusion of claim 26 wherein said discovering step includes the steps of:

transmitting a discovery request frame, said discovery request frame having a security feature group address;

receiving a discovery response frame from each security-enabled interconnect device;

building and maintaining an interconnect device list of each security-enabled interconnect device that transmitted said discovery response frame back to said managed hub.

28. The method for providing security against intrusion of claim 27 wherein said detecting step includes the steps of:

comparing, for each port, a source address of a station attempting to connect to said port with an authorized address list of addresses for said port and determining whether said source address is on said authorized address list.

29. The method for providing security against intrusion of claim 27 wherein following said disabling step said method further includes:

sending a trap frame to a network management station indicating that an intrusion has been detected on said first port; and

transmitting a security breach detected frame having said security feature group address to each security-enabled interconnect device that has an entry in said interconnect device list.

30. The method for providing security against intrusion of claim 26 wherein following said reenabling step said managed hub sends a trap frame to a network management station indicating that said filtering step has been completed.

31. An apparatus for providing security against intrusion in a managed hub of a computer network having at least one interconnect device, said apparatus comprising:

means for building and maintaining an authorized address list of addresses that are allowed to connect to each port;

means for discovering each interconnect device that is enabled to provide network security;

means for detecting an unauthorized address on a first port and means for disabling said first port;

means for notifying each security-enabled interconnect device that the unauthorized address has been detected on said first port; and

means for reenabling said first port after each security-enabled interconnect device has notified said managed hub that a filter has been set to prevent frames with the unauthorized address from flowing through each security-enabled interconnect device.

32. The apparatus for providing security against intrusion of claim 31 wherein said means for discovering includes:

means for transmitting a discovery request frame, said discovery request frame having a security feature group address;

means for receiving a discovery response frame from each security-enabled interconnect device;

means for building and maintaining an interconnect device list of each security-enabled interconnect device that transmitted said discovery response frame back to said managed hub.

33. The apparatus for providing security against intrusion of claim 32 wherein said means for detecting includes:

means for comparing, for each port, a source address of a station attempting to connect to said port with an authorized address list of addresses for said port and means for determining whether said source address is on said authorized address list.

34. The apparatus for providing security against intrusion of claim 32 further including:

means for sending a trap frame to a network management station indicating that an intrusion has been detected on said first port; and

means for transmitting a security breach detected frame having said security feature group address to each security-enabled interconnect device that has an entry in said interconnect device list.

35. The apparatus for providing security against intrusion of claim 31 wherein said managed hub further comprises means for sending a trap frame to a network management station indicating that said filter has been set at each security-enabled interconnect device.

* * * * *

United States Patent [19]
Klaus

[11] **Patent Number:** **5,892,903**
[45] **Date of Patent:** **Apr. 6, 1999**

[54] **METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM**

[75] Inventor: **Christopher W. Klaus**, Atlanta, Ga.

[73] Assignee: **Internet Security Systems, Inc.**, Atlanta, Ga.

[21] Appl. No.: **710,162**

[22] Filed: **Sep. 12, 1996**

[51] **Int. Cl.**^{6} **G06F 11/00**
[52] **U.S. Cl.** **395/187.01**; 395/200.57
[58] **Field of Search** 395/187.01, 186, 395/188.01, 200.59, 200.57, 183.04, 200.67, 200.68

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,223,380	9/1980	Antonaccio et al.	364/200
5,204,966	4/1993	Wittenberg et al.	395/188.01
5,309,562	5/1994	Li	395/200
5,311,593	5/1994	Carmi	380/23
5,347,450	9/1994	Nugent	395/200
5,371,852	12/1994	Attanasio et al.	395/200
5,515,508	5/1996	Pettus et al.	395/200.01
5,557,742	9/1996	Smaha et al.	395/186
5,623,601	4/1997	Vu	395/187.01

OTHER PUBLICATIONS

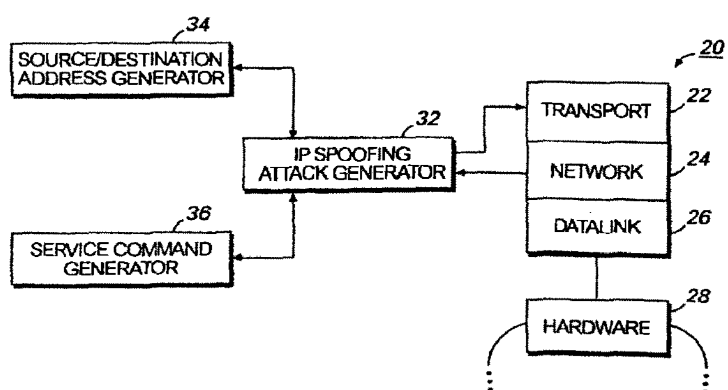
Guha et al., "Network Security via Reverse Engineering of TCP Code: Vulnerability Analysis and Proposeed Solutions", IEEE, pp. 603–610, Mar. 1996.
Garg et al., "High Level Communication Primitives for Concurrent Systems", IEEE, pp. 92–99, 1988.
Hastings et al., "TCP/IP Spoofing Fundamentals", IEEE, pp. 218–224, May 1996.
Snapp, "Signature Analysis and Communication Issues in a Distributed Intrusion Detection System", Master Thesis; University of California, Davis, CA, pp. 1–40, 1991.
Guha et al., "Network Security via Reverse Engineering of TCP Code: Vulnerability Analysis and Proposed Solutions", IEEE, pp. 40–48, Jul. 1997.
Djahandari et al., "An MBone Proxy for an Application Gateway Firewall", IEEE, pp. 72–81, Nov. 1997.
Kim et al., "Implementing a Secure rlogin Environment: A Case Study of Using a Secure Network Layer Protocol", Department of Computer Science, University of Arizona, pp. 1–9, Jun. 1995.
Satyanarayanan, "Integrating Security in a Large Distributed System", Acm Transactions on Computer Systems, vol. 7, No. 3, pp. 47–280, Aug. 1989.

Primary Examiner—Albert Decady
Assistant Examiner—Scott T. Badesman
Attorney, Agent, or Firm—Morris, Manning & Martin, L.L.P.

[57] **ABSTRACT**

A system and method is disclosed for detecting security vulnerabilities in a computer network. The system includes an IP spoofing attack detector, a stealth port service map generator, a source port verifier, source routing verifier, an RPC service detector and a Socks configuration verifier. Each of these verifiers may be operated separately or as a group to detect security vulnerabilities on a network. Each verifier may be programmed to exhaustively test all ports of all computers on a network to detect susceptibility to IP spoofing attacks, access to services with little or no authorization checks or misconfigured routers or Socks servers. The detected vulnerabilities or the location of services having little or no authorization checks may be stored in a table for reference by a network administrator. The service map generated by the stealth service map generator may be used to identify all service ports on a network to facilitate the operation of the other verifiers which send service command messages to service ports to detect their accessibility. A graphic user interface (GUI) may be used to provide input and control by a user to the security verifiers and to present options and display information to the user.

41 Claims, 8 Drawing Sheets



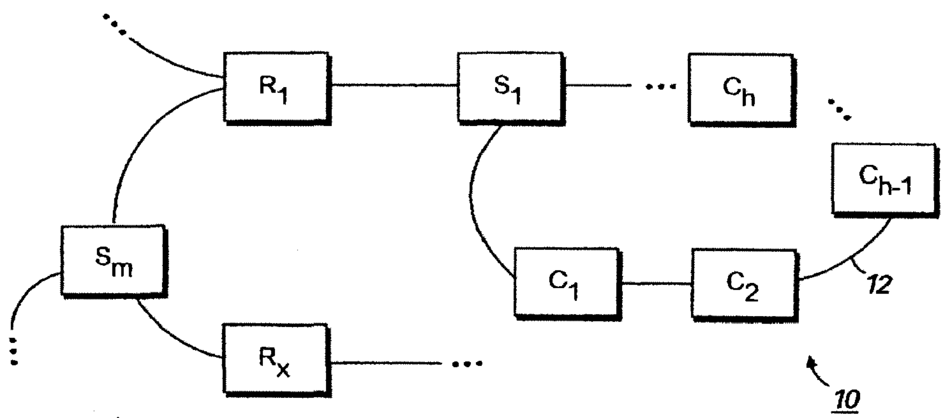

R1
S1
Ch
Ch-1
Sm
C1
C2
12
Rx
10

FIG.1

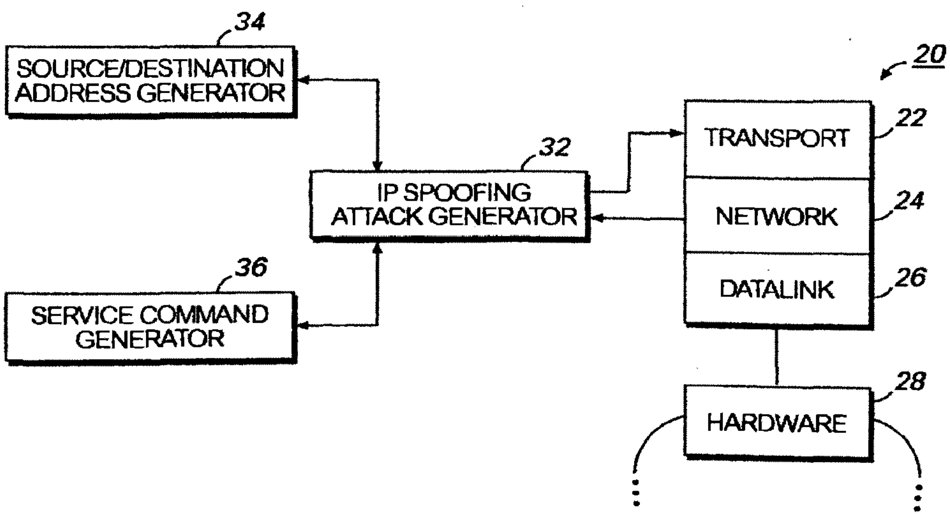

34
SOURCE/DESTINATION ADDRESS GENERATOR
20
TRANSPORT
22
32
IP SPOOFING ATTACK GENERATOR
NETWORK
24
36
DATALINK
26
SERVICE COMMAND GENERATOR
28
HARDWARE

FIG.2

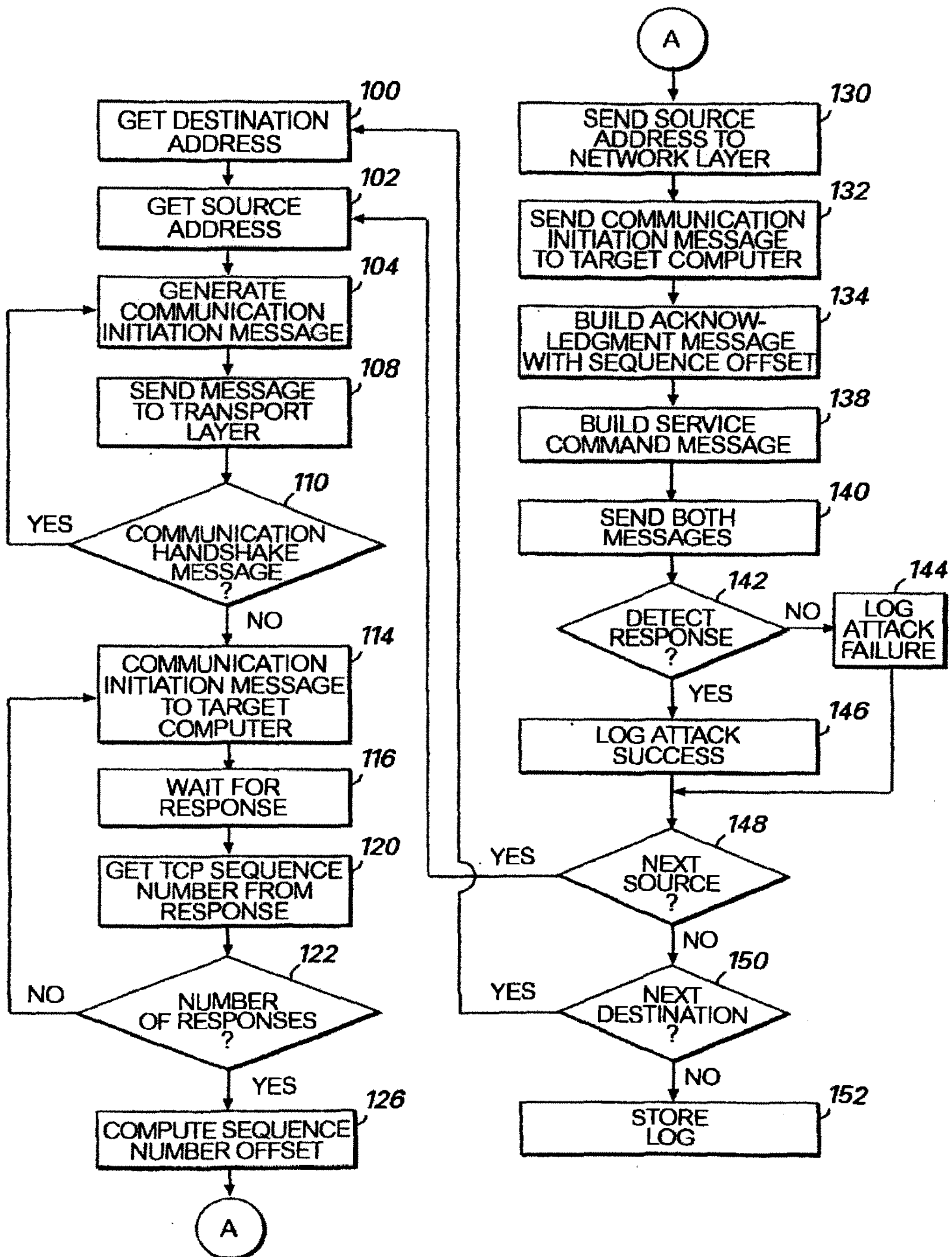

A
GET DESTINATION ADDRESS
100
GET SOURCE ADDRESS
102
GENERATE COMMUNICATION INITIATION MESSAGE
104
SEND MESSAGE TO TRANSPORT LAYER
108
COMMUNICATION HANDSHAKE MESSAGE ?
110
YES
NO
COMMUNICATION INITIATION MESSAGE TO TARGET COMPUTER
114
WAIT FOR RESPONSE
116
GET TCP SEQUENCE NUMBER FROM RESPONSE
120
NUMBER OF RESPONSES ?
122
NO
YES
COMPUTE SEQUENCE NUMBER OFFSET
126
A
SEND SOURCE ADDRESS TO NETWORK LAYER
130
SEND COMMUNICATION INITIATION MESSAGE TO TARGET COMPUTER
132
BUILD ACKNOW-LEDGMENT MESSAGE WITH SEQUENCE OFFSET
134
BUILD SERVICE COMMAND MESSAGE
138
SEND BOTH MESSAGES
140
DETECT RESPONSE ?
142
NO
LOG ATTACK FAILURE
144
YES
LOG ATTACK SUCCESS
146
NEXT SOURCE ?
148
YES
NO
NEXT DESTINATION ?
150
YES
NO
STORE LOG
152

FIG.3

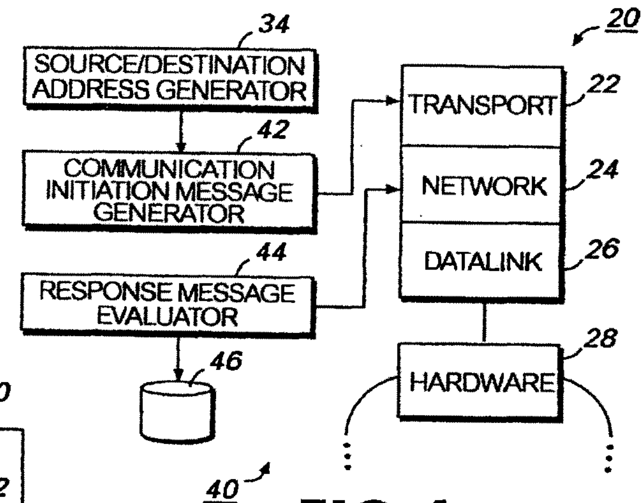

34
SOURCE/DESTINATION ADDRESS GENERATOR
42
COMMUNICATION INITIATION MESSAGE GENERATOR
44
RESPONSE MESSAGE EVALUATOR
46
20
TRANSPORT
22
NETWORK
24
DATALINK
26
HARDWARE
28
40

FIG.4

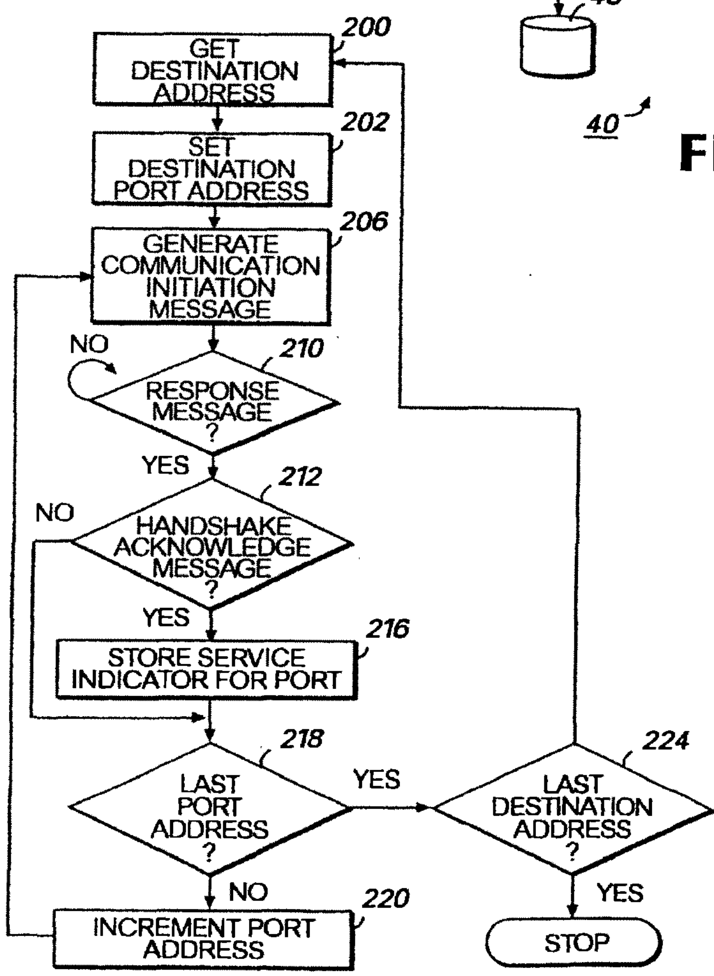

GET DESTINATION ADDRESS
200
SET DESTINATION PORT ADDRESS
202
GENERATE COMMUNICATION INITIATION MESSAGE
206
NO
RESPONSE MESSAGE ?
210
YES
HANDSHAKE ACKNOWLEDGE MESSAGE ?
212
NO
YES
STORE SERVICE INDICATOR FOR PORT
216
LAST PORT ADDRESS ?
218
YES
NO
INCREMENT PORT ADDRESS
220
LAST DESTINATION ADDRESS ?
224
YES
STOP

FIG.5

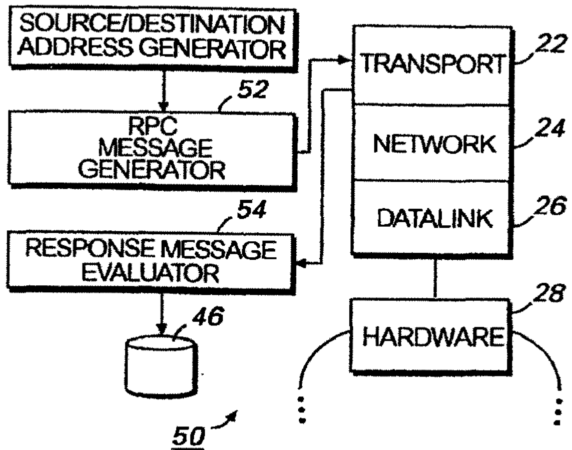

SOURCE/DESTINATION ADDRESS GENERATOR
52
RPC MESSAGE GENERATOR
54
RESPONSE MESSAGE EVALUATOR
46
50
TRANSPORT
22
NETWORK
24
DATALINK
26
HARDWARE
28

FIG.6

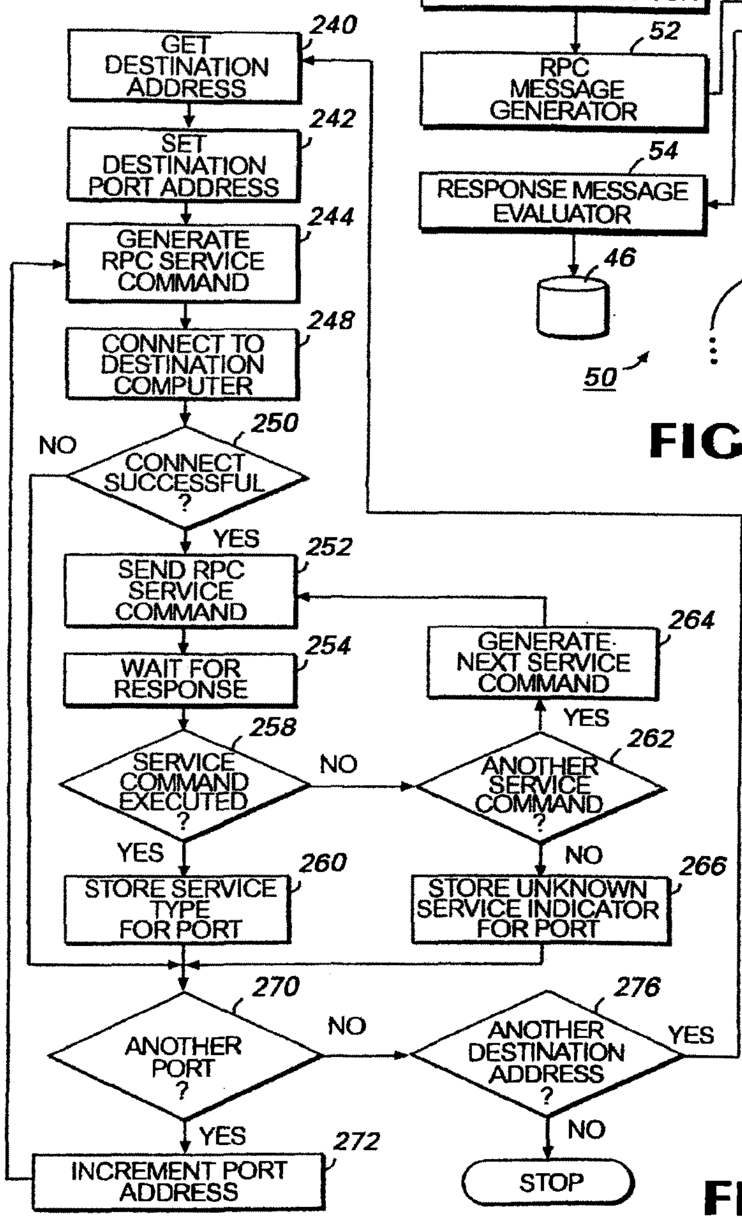

GET DESTINATION ADDRESS
240
SET DESTINATION PORT ADDRESS
242
GENERATE RPC SERVICE COMMAND
244
CONNECT TO DESTINATION COMPUTER
248
CONNECT SUCCESSFUL ?
250
NO
YES
SEND RPC SERVICE COMMAND
252
WAIT FOR RESPONSE
254
SERVICE COMMAND EXECUTED ?
258
NO
YES
STORE SERVICE TYPE FOR PORT
260
ANOTHER SERVICE COMMAND ?
262
YES
NO
GENERATE NEXT SERVICE COMMAND
264
STORE UNKNOWN SERVICE INDICATOR FOR PORT
266
ANOTHER PORT ?
270
NO
YES
INCREMENT PORT ADDRESS
272
ANOTHER DESTINATION ADDRESS ?
276
YES
NO
STOP

FIG.7

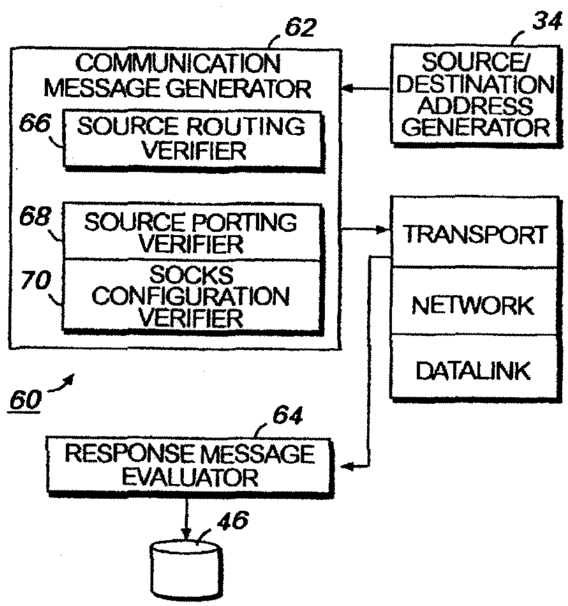

62
COMMUNICATION MESSAGE GENERATOR
66
SOURCE ROUTING VERIFIER
68
SOURCE PORTING VERIFIER
70
SOCKS CONFIGURATION VERIFIER
34
SOURCE/ DESTINATION ADDRESS GENERATOR
TRANSPORT
NETWORK
DATALINK
60
64
RESPONSE MESSAGE EVALUATOR
46

FIG.8

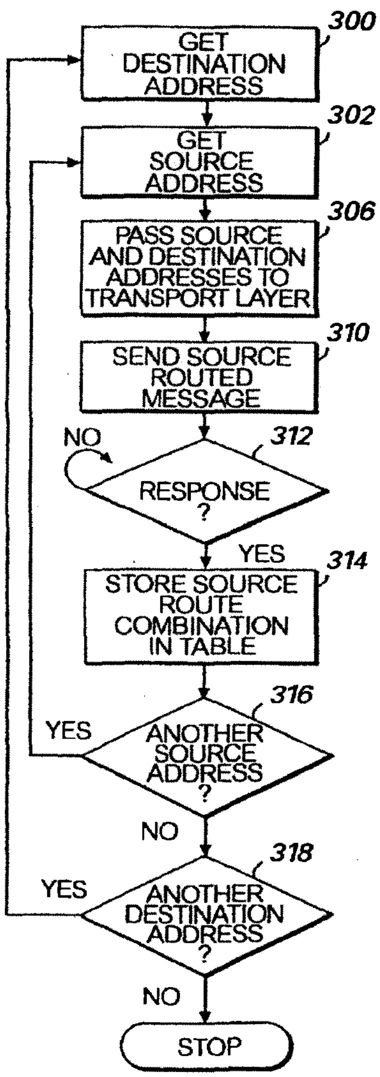

300
GET DESTINATION ADDRESS
302
GET SOURCE ADDRESS
306
PASS SOURCE AND DESTINATION ADDRESSES TO TRANSPORT LAYER
310
SEND SOURCE ROUTED MESSAGE
312
NO
RESPONSE ?
YES
314
STORE SOURCE ROUTE COMBINATION IN TABLE
316
YES
ANOTHER SOURCE ADDRESS ?
NO
318
YES
ANOTHER DESTINATION ADDRESS ?
NO
STOP

FIG.9

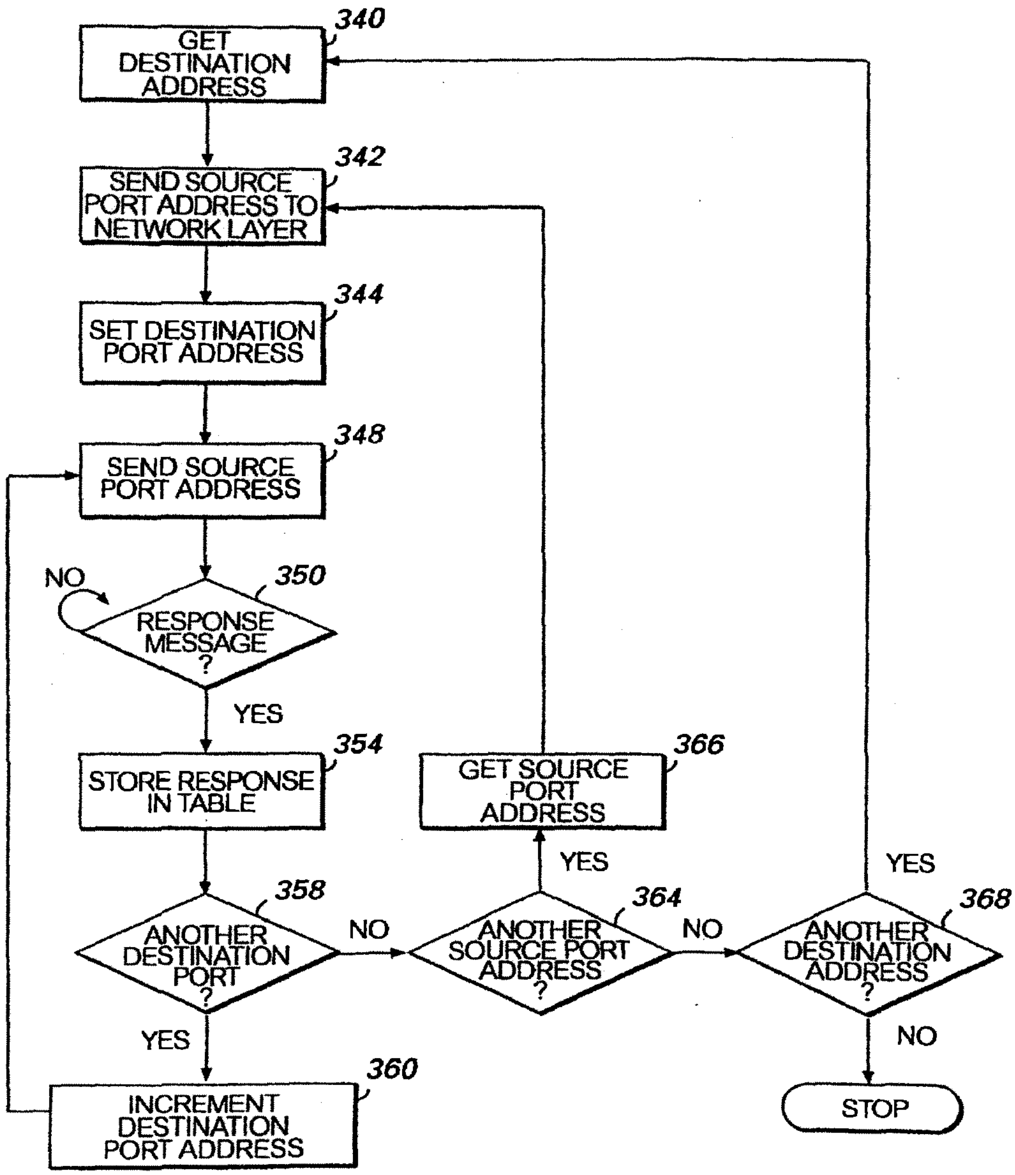

340
GET DESTINATION ADDRESS
342
SEND SOURCE PORT ADDRESS TO NETWORK LAYER
344
SET DESTINATION PORT ADDRESS
348
SEND SOURCE PORT ADDRESS
350
RESPONSE MESSAGE ?
NO
YES
354
STORE RESPONSE IN TABLE
358
ANOTHER DESTINATION PORT ?
YES
NO
360
INCREMENT DESTINATION PORT ADDRESS
364
ANOTHER SOURCE PORT ADDRESS ?
YES
NO
366
GET SOURCE PORT ADDRESS
368
ANOTHER DESTINATION ADDRESS ?
YES
NO
STOP

FIG.10

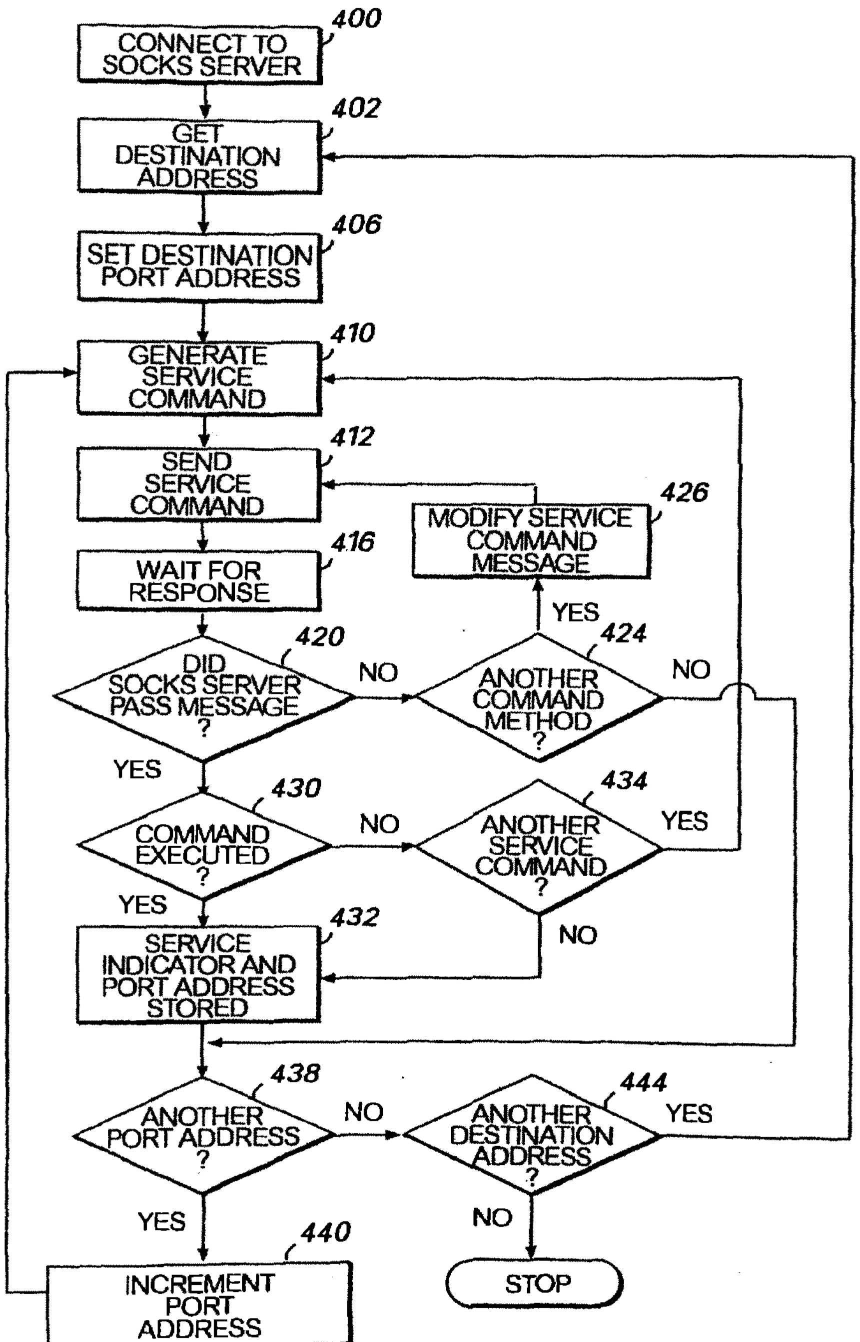

400
CONNECT TO SOCKS SERVER
402
GET DESTINATION ADDRESS
406
SET DESTINATION PORT ADDRESS
410
GENERATE SERVICE COMMAND
412
SEND SERVICE COMMAND
426
MODIFY SERVICE COMMAND MESSAGE
416
WAIT FOR RESPONSE
YES
424
420
DID SOCKS SERVER PASS MESSAGE ?
NO
ANOTHER COMMAND METHOD ?
NO
YES
430
COMMAND EXECUTED ?
NO
434
ANOTHER SERVICE COMMAND ?
YES
YES
432
SERVICE INDICATOR AND PORT ADDRESS STORED
NO
438
ANOTHER PORT ADDRESS ?
NO
444
ANOTHER DESTINATION ADDRESS ?
YES
YES
440
INCREMENT PORT ADDRESS
NO
STOP

FIG.11

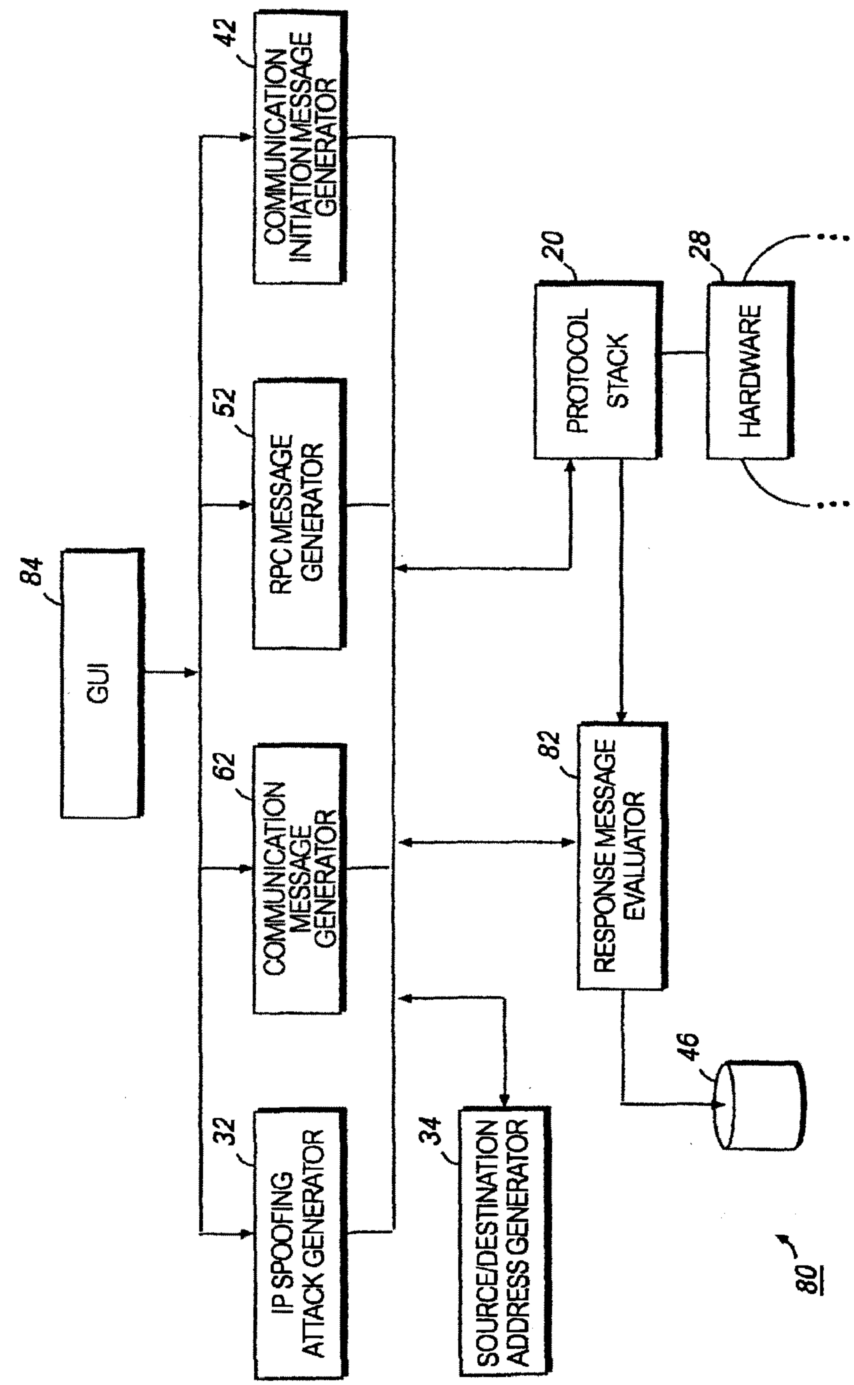

COMMUNICATION INITIATION MESSAGE GENERATOR
42
RPC MESSAGE GENERATOR
52
GUI
84
COMMUNICATION MESSAGE GENERATOR
62
IP SPOOFING ATTACK GENERATOR
32
SOURCE/DESTINATION ADDRESS GENERATOR
34
PROTOCOL STACK
20
HARDWARE
28
RESPONSE MESSAGE EVALUATOR
82
46
80

FIG.12

METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM

FIELD OF THE INVENTION

This invention relates to network communications for computers, and, more particularly, to computer communications over open networks.

BACKGROUND OF THE INVENTION

Many business and scientific organizations in the United States which use more than one computer in their operations couple the computers together through a network. The network permits the computers to be islands of processing which may share resources or data through communication over the network. The data which may be communicated over the network may take the form of programs developed on a user's computer, data files created on a user's computer, electronic mail messages and other data messages and files which may be generated or modified by a user at a user's computer. Typically, the user's computer includes an operating system for controlling the resources of the user's computer, including its central processing unit ("CPU"), memory (both volatile and non-volatile memory) and computer peripherals such as printers, modems and other known computer peripheral devices. The user typically executes application programs and system services to generate data files or programs.

Most computers are coupled to a network through a network communication printed circuit card which is typically resident within each computer system. This communication card typically includes processors, programs and memory to provide the electrical signals for transmission of data and implement the protocol which standardizes the messages transmitted through a network. To communicate data from a user's application program or operating system service, a protocol stack is typically implemented between the communication card for the network and the operating system services and application programs.

The typical protocol stack used on most open networks is a Transport Control Protocol/Internet Protocol ("TCP/IP"). This protocol stack includes a transport layer which divides a data stream from an application program or service into segments and which adds a header with a sequence number for each segment. The TCP segments generated by the transport layer are passed to the Internet Protocol ("IP") layer. The IP layer creates a packet having a packet header and a data portion. The data portion contains the TCP segment and the packet header contains a source address identifying the computer sending a message and a destination address identifying the computer for which the message is intended. The IP layer also determines the physical address of the destination computer or an intermediate computer, in some cases, which is intended to receive the transmitted message. The packet and the physical addresses are passed to a datalink layer. The datalink layer typically is part of the program implemented by a processor on the communication card and it encapsulates the packet from the IP layer in a datalink frame which is then transmitted by the hardware of the communication card. This datalink frame is typically called a packet. For purposes of this specification, the word "message" includes the data entities packet and datalink frame.

At the destination computer, the communication card implements the electrical specification of a hardware communication standard, such as Ethernet, and captures a data message from a source computer. The datalink layer at the destination computer discards the datalink header and passes the encapsulated packet to the IP layer at the destination computer. The IP layer at the destination computer verifies that the packet was properly transmitted, usually by verifying a checksum for the packet. The IP layer then passes the encapsulated TCP segment to the transport layer at the destination computer. The transport layer verifies the checksum of the TCP message segment and the sequence number for the TCP packet. If the checksum and TCP sequence number are correct, data from the segment is passed to an application program or service at the destination computer.

Segregation of communication functions in the various layers of the protocol stack and the segregation of the protocol stack from the communication card and application programs, modularizes the functions required to implement communication over a computer network. This modularization of functions simplifies computer communication operation and maintenance. It also does not require a user to have knowledge of how the protocol stack and communication card communicate in order to send data messages to other computers over the network.

All of the computers coupled to a network may have approximately the same resources available at each machine. The type of network is sometimes called a peer to peer network. Another type of network environment is one in which one computer controls shared databases and other computer resources with other computers over the network. The computer controlling access to the shared resources is typically called a server and the computers utilizing the shared resources are called clients.

In both the client/server and peer to peer environments, a server or computer may be used as a gateway to other networks or computers. Another device which a message may encountered as it moves along a network is a router. A router examines destination addresses of messages it receives and routes them in an efficient manner to the specified destination computer. For example, a server on a first network may be coupled to a router which is coupled to a plurality of servers including a server on a second network and a server for a third network. In this type of environment, the computer on the first network may communicate with a computer on the third network by generating data messages which have the destination address for a computer on the third network. The message circulates through the first network and is eventually provided to the server of the first network. The server of the first network then passes the message to the router which determines that the message is addressed for the third network. Accordingly, it sends the message to the server of the third network. The communication facilities at the server for the third network recognize the destination address as existing on the third network and pass the message to a computer on the third network where it eventually would be passed to the destination computer.

While this type of communication effectively and efficiently couples all of the computers from all of the networks together without requiring a message to pass through each computer on the network, a message typically passes through a number of computers, routers, servers or gateways prior to reaching the destination computer. As a result, the data messages from one computer to another computer may be intercepted and data obtained from the message as the message is passed on to another computer. The type of network wherein this type of accessible communication is provided is typically called an open network. One of the more popularly known open networks is the Internet where literally millions of servers and computers are coupled through a TCP/IP communication protocol.

While the open network architecture of the Internet permits a user on a network to have access to information on many different computers, it also provides access to messages generated by a user's computer and to the resources of the user's computer. In fact, there are persons who attempt to use knowledge regarding the operations of the protocol stack and operating systems in an effort to gain access to computers without authorization. These persons are typically called "hackers". Hackers present a significant security risk to any computer coupled to a network where a user for one computer may attempt to gain unauthorized access to resources on another computer of the network. For example, an employee may attempt to gain access to private and confidential employee records on a computer used by the human resources department of an employer.

In an effort to control access to a network and, hence, limit unauthorized access to computer resources available on that network, a number of computer communication security devices and techniques have been developed. One type of device which is used to control the transfer of data is typically called a "firewall". Firewalls are routers which use a set of rules to determine whether a data message should be permitted to pass into or out of a network before determining an efficient route for the message if the rules permit further transmission of the message. In this specification the term "routers" includes firewalls and routers.

In the TCP/IP protocol, a communication connection is established through a three handshake open network protocol. The first handshake or data message is from a source computer and is typically called a "synchronization" or "sync" message. In response to a sync message, the destination computer transmits a synchronization-acknowledgment ("sync-ack") message. The source computer then transmits an acknowledgment ("ack") message and a communication connection between the source and destination computer is established. To limit access to computers on a network, routers may be provided as a gateway to the network and programmed to detect and block sync messages being transmitted from a computer external to the network to a destination computer on the network. That is, computers on the network may send out sync messages through the router to initiate communication with other computers, but computers outside the router and its network cannot send sync messages through the router to initiate communication with computers on the network. In this way, a hacker cannot attempt to initiate communication with a computer on the network.

Hackers, however, have developed other ways which may be helpful in bypassing the screening function of a router. For example, one computer, such as a server on the network, may be permitted to receive sync messages from a computer outside the network. In an effort to get a message to another computer on a network, a hacker may attempt to use source routing to send a message from the server to another computer on the network. Source routing is a technique by which a source computer may specify an intermediate computer on the path for a message to be transmitted to a destination computer. In this way, the hacker may be able to establish a communication connection with a server through a router and thereafter send a message to another computer on the network by specifying the server as an intermediate computer for the message to the other computer.

In an effort to prevent source routing techniques from being used by hackers, some routers may be configured to intercept and discard all source routed messages to a network. For a router configured with source routing blocking, the router may have a set of rules for inbound messages, a set of rules for outbound messages and a set of rules for source routing messages. When a message which originated from outside the network is received by such a router, the router determines if it is a source routed message. If it is, the router blocks the message if the source routing blocking rule is activated. If blocking is not activated, it allows the source routed message through to the network. If the message is not a source routed message, the router evaluates the parameters of the message in view of the rules for receiving messages from sources external to the network. One such rule is the external sync message filter discussed above. Other rules may also be implemented in such a router. However, a router vulnerability exists where the rules used by the router are only compared to messages that are not source routed and the source routed blocking rule is not activated. In this situation, the router permits source routed messages through without comparing them to the filtering rules. In such a case, a computer external of the network may be able to bypass the external sync message filter and establish a communication connection with a computer on the network by using source routed messages.

What is needed is a system and method for verifying that the source routing blocking feature of a router has been activated.

Networks may also be coupled to external computers through a specialized communication filter typically known as a "Socks" proxy server. A Socks proxy server is interposed between a network and external computers. For an external computer to establish communication with a computer on a network coupled to a Socks server, the external computer first establishes a communication connection with the Socks server and the Socks server establishes a communication connection with the destination computer. Thereafter, the Socks server relays messages between the external computer and a computer on the network only if they comply with the filter rules configured for the Socks server. Typically, Socks servers are used to interface e-mail, File Transfer Protocol ("FTP") and Telnet communication services between computers on a network and computers external of the network and to block access to most other ports on a network. The interrogation and evaluation of messages through a Socks server is dependent upon the network administrator for proper configuration. Known methods for verifying the configuration of the Socks server is to view the configuration files of the Socks server to verify the rules are properly set. However, this method does not ascertain the rules actually being implemented by the Socks server.

What is needed is a method and system for determining the rules being implemented by a Socks server without reviewing the configuration files for a Socks server.

Another entry port for hackers are commonly known services which provide information to external users without requiring authorization checks such as passwords. Most implementations of the UNIX operating system, for example, include Remote Procedure Call (RPC) services which may not be protected by authorization checks. The ports on which RPC services are located may be determined by querying a UNIX operating system service known as "portmapper". In an effort to obtain knowledge regarding accessible services on a computer, a hacker may make an inquiry of the portmapper service at its port in order to obtain information regarding the RPC services available for entry on the computer. Although the portmapper service may be reconfigured to include an authorization check that still does not provide an authorization check for the RPC services themselves.

What is needed is a system and method for detecting and reporting to a network administrator those ports which are coupled to RPC services which have little or no authorization checks.

As discussed above, the transport layer of the protocol stack provides a sequence number for each data segment to be transmitted. In the TCP/IP protocol, the sequence number is called a TCP sequence number which is placed in the TCP header generated by the transport layer. The sequence number for the data segment is typically incremented at predefined time units, for example, each second, and for each communication connection or attempted communication connection. For example, in attempting to establish communication with another computer on a TCP/IP network, the source computer generates a sync message with a TCP sequence number. The destination computer responds with a sync/ack message where the ack value in the message is the sequence number from the received sync message and the sequence number for the destination computer is a number generated by the destination computer. This sequence number typically has the value of the last TCP sequence number generated by the destination computer plus the addition of a preferred offset value for each predefined time unit and communication connection that has occurred since the last TCP sequence number was generated. The ack message from the source computer to the destination computer which completes the communication connection must include the TCP sequence number received from the destination computer in the sync/ack message.

One known way which hackers attempt to access a computer on a network is to emulate the communication of messages from another computer on the network. A hacker emulates another computer on the network by first blocking a communication port on the computer being emulated by repeatedly sending sync messages to a port on the computer. This causes the communication program for the port to fill its communication buffer with half-open communication connections. When the buffer is full, no more sync messages are accepted until the oldest attempted half-open communication connection times out. Typically, the time out period is ten minutes or longer. In order to obtain a sequence number, the hacker's computer sends a number of sync messages to the computer which is the target of the attack which responds with a plurality of sync/ack messages containing TCP sequence numbers to the hacker's computer. The TCP sequence numbers from the sync/ack messages may be compared to statistically determine the offset used by the target computer to generate TCP sequence numbers. The hacker then uses the emulated computer's blocked port address as the source computer address for a sync message originated by the hacker's computer. In response, the target computer replies with a sync/ack message which is addressed to the blocked computer port of the emulated computer. Thus, the hacker's computer does not receive the sync/ack message with the TCP sequence number required for a proper response. However, the hacker's computer then sends an ack message with the next computed sequence number derived from bombarding the target computer with sync messages. If the sequence number has been correctly computed so that it matches the sequence number in the sync/ack message sent by the target computer to the blocked computer port, a communication connection is established and the hacker is able to transmit a command to the service on the port of the target computer through which communication has been established. In a UNIX system, a hacker normally attacks the ports coupled to the rsh and rlogin services since the authorization check for these services is usually the source address. If the hacker is able to successfully emulate a computer on the network having an address authorized for the service on the target computer port, the command is executed by the service. The service command typically provided to the port of the target computer disrupts the target computer's operation so the hacker's computer has unencumbered access to the target computer's resources. These types of attacks which use predicted TCP sequence numbers are typically known as IP spoofing attacks.

Although the protocol stack for each computer uses different offset values to generate the initial TCP sequence number for establishing communication links, some machines generate initial sequence numbers which are more easily predicted than others. What is needed is a way of detecting which computers on a network are susceptible to attacks using predicted TCP sequence numbers.

SUMMARY OF THE INVENTION

The above-noted vulnerabilities of a computer network may be automatically detected by a computer program which implements the system and method of the present invention. One embodiment of the present invention includes an Internet protocol ("IP") spoofing attack generator for generating an IP spoofing attack directed to a target computer and a service command message generator for sending a command to be executed by a service coupled to a port on the target computer so that in response to the target computer being compromised by the IP spoofing attack the target computer generates a compromise indicator without altering or destroying the target computer's services and/or operations. Preferably, the target computer response is an electronic mail message or a Telnet initiation message. Preferably, the IP spoofing attack is directed against a port coupled to the rsh or rlogin services. Preferably, the embodiment includes a source/destination address generator which generates source and destination addresses for messages corresponding to an open network protocol. The destination addresses correspond to the target computer and the source addresses correspond to the emulated computer in the IP spoofing attack. The source/destination address generator generates the address for each computer on a network so that an IP spoofing attack from every computer on the network is directed against each of the other computers on the network. In this manner, those computers on the network which are most susceptible to an IP spoofing attack may be detected and modification of the TCP sequence number generator in the protocol stack may be adjusted to make an IP spoofing attack less likely to succeed.

Another embodiment of the present invention for detecting security vulnerabilities in the configuration rules of a router includes a communication message generator for generating and sending communication messages to computers coupled through an open network to a router and a response message detector for detecting responses from computers on the network generated in response to the communication messages. This embodiment of the present invention detects the vulnerability of the router to pass communication messages to computers on the network. Depending on the type of communication or service command message to which a computer responds, the inventive system may determine rules not implemented by a router. In one preferred embodiment, the communication message generator includes a Socks configuration verifier which establishes a communication connection with a Socks server and attempts to send service command messages for different services with source addresses for computers on the network. The responses of the destination computer are examined to determine the types of messages which the Socks server passes to computers on the network from computers external to the network. This system may be used to verify the rules actually implemented by a Socks server.

In another embodiment, the communication message generator includes a source porting verifier which sets the source port address in a header for a generated communication message to a predetermined value to see if the router passes externally generated messages having the specified source port address to the network. Preferably, the predetermined value is the default source port identifier for a service having a known required predetermined source port address such as an FTP service. In this manner, the system of the present invention detects whether a computer external of the network can establish a communication connection with a computer on the network by using a predetermined source port identifier to avoid other rules in a router.

In another embodiment of the present invention, the communication message generator includes a source routing verifier which generates source-routed communication messages to determine whether the router has a source router message blocking rule activated. This embodiment may be used to determine whether the rules that the router applies to communication messages originated by computers external to the network may be bypassed by using source routed messages.

In another embodiment of the present invention, an RPC message generator generates RPC service command messages which are sent to ports of computers on a network to detect the ports coupled to RPC services having little or no authorization checks. These ports and the coupled services, if determined, may be stored and provided to a network administrator for installing more rigorous authorization checks.

In another embodiment of the present system, a communication initiation message generator for generating communication initiation messages for a three handshake protocol and a response message evaluator are used to determine which of the ports on each computer in a network have a service coupled thereto. This inventive system operates by sending sync messages to each port on every computer on the network and building a table of service identifiers which identify those ports which responded with a message indicating the presence of a service. Preferably, the communication initiation message is a sync message for TCP/IP networks and the messages indicating a service is coupled to a port is a sync/ack message. In this manner, the inventive system may build a map of those ports of each computer on the network which have service coupled thereto without creating a log of any communication connections on any the computers on the network. Since communication connections are only established and logged when the originating computer sends the ack message, this embodiment generates a map of available services in a stealth manner. This embodiment of the inventive system may be coupled with one or more of the other embodiments which generate service command messages to eliminate ports from the attempts to detect vulnerable services. Such a system speeds the security analysis of a network.

These and other advantages and benefits of the present invention may be ascertained from reading of the detailed specification in conjunction with the drawings.

DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated and constitute a part of this specification, illustrate a number of embodiments of the invention and, together with the general description given above, and the detailed description of the embodiments given below, serve to explain the principles of the invention.

FIG. 1 is a schematic of an open network system;

FIG. 2 is a block diagram of an embodiment of the present invention used to detect IP spoofing attack vulnerability;

FIG. 3 is a flow chart of the preferred process implemented by the embodiment depicted in FIG. 2;

FIG. 4 is a block diagram of an embodiment of the present invention used to map the ports of computers of a network which are coupled to services without generating communication connections;

FIG. 5 is a flow chart of the preferred process implemented by the embodiment depicted in FIG. 4;

FIG. 6 is a block diagram of an embodiment of the present invention used to detect Remote Procedure Call (RPC) services available on a network which have little or no authorization checks;

FIG. 7 is a flow chart of the preferred process implemented by the embodiment shown in FIG. 6;

FIG. 8 is a block diagram of an embodiment of the present invention used to verify the configuration of routers and/or Socks servers;

FIG. 9 is a flow chart of the preferred process implemented by the source routing verifier of FIG. 8;

FIG. 10 is a flow chart of the preferred process implemented by the source porting verifier of FIG. 8;

FIG. 11 is a flow chart of the preferred process implemented by the Socks server verifier of FIG. 8; and

FIG. 12 is a block diagram of a preferred embodiment of the present invention which incorporates the components of the systems shown in FIGS. 2, 4, 6 and 8.

DETAILED SPECIFICATION OF EMBODIMENTS OF THE INVENTION

An open network system in which a system made in accordance with the principles of the present invention may be used is shown in FIG. 1. An internetwork 10 may be comprised of a network 12 which in turn may be coupled to other servers, gateways and routers. Network 12 includes a plurality of computers C_1–C_n which are coupled through network 12 to a server S_1. This network in turn may be coupled to a router R_1 to provide further secured computer communication with other servers represented by S_m or other routers labeled R_x as shown in FIG. 1. Although the principles of the present invention are extensible to other protocols, the invention is preferably used on networks which utilize the TCP/IP protocol. The computer program implementing a system or method of the present invention may reside on any of the computers on the network 12 or any server or any router of internetwork 10.

Structure of a system embodiment made in accordance with the principles of the present invention is shown in FIG. 2. A computer executing a program implementing the system or method of the present invention would typically include the programs and communication hardware card which implement a protocol stack 20. Protocol stack 20 is comprised of transport layer 22, network layer 24 and datalink layer 26. These layers of protocol stack 20 operate in the well-known manner set forth above. The data frame prepared by datalink layer 26 is passed to communication hardware 28 for transmission to other computers in accordance with the source and destination information provided in the various headers generated by protocol stack 20.

In one embodiment of the present invention which detects a computer's vulnerability to IP spoofing, the system includes an IP spoofing attack generator 32, a source/destination address generator 34 and a service command generator 36. Source/destination address generator 34 identifies the internet and physical addresses of the computers on the network 12 to be tested. Source/destination address generator 34 verifies that each computer on network 12 is emulated in IP spoofing attacks on all of the other computers on network 12. In this manner, the inventive system exhaustibly tests all possible attack combinations on a network. Service command generator 36 generates commands for a service which may be coupled to a port which IP spoofing attack generator 32 is able to initiate a communications connection. Preferably, service command generator 36 generates commands for services which have little or no authorization checks. "Little" means that the authorization check verifies a computer address is on the network 12 or the like while "no" authorization check means the service executes any valid server command received on a port regardless of originating source. Preferably, service commands are generated for electronic mail, file transport protocol (FTP) and Telnet services. These commands preferably indicate that a target computer identified by a destination address has been compromised without altering the target computer's operational parameters such as changing system privileges for a user or deleting data files. Examples of such commands include a Telnet session initiation command such as telnet attack_computer_address where attack_computer_address is the address of the computer which performed the IP spoofing attack on the target computer. Another example of such a message is mail admin message where admin indicates the system or network administrator's mailbox and message indicates the contents of the message informing the administrator of the compromise. The service command received from command message generator 36 and the source and destination addresses received from source/destination address generator 34 are used by IP spoofing attack generator 32 to provide data and header content for messages sent to transport layer 22 and network layer 24 of protocol stack 20 which are used to implement the IP spoofing attack and detection.

The process implemented by IP spoofing attack generator 36 is shown in FIG. 3. That process begins by obtaining a destination address (Block 100) and a source address (Block 102) from source/destination address generator 34. Attack generator 32 then generates a communication initiation message for a three handshake protocol which is preferably a synchronization or sync message for the TCP/IP protocol (Block 104). The communication initiation message is sent to a port on the source address computer by placing the message in a TCP segment and passing it to the transport layer (Block 108). Transport layer 22, network layer 24 and datalink layer 26 all appropriately encapsulate the sync message for transmission to the computer at the source address which is the address of the computer to be emulated in the IP spoofing attack. The process awaits the reception of a handshake acknowledgment message from the computer at the source address (Block 110). The handshake acknowledgment message in the TCP/IP protocol is a sync/ack message. If a sync/ack message is received, another sync message is generated and sent to the same port address of the computer at the source address. This process continues until no sync/ack message is received from the computer at the source address within a predetermined time. These steps are performed to fill the communication buffer for a port on the source address computer with half-opened communication connections. This full buffer condition exists until the time period for completing a communication connection expires. In most computers, the expiration period is at least 10 minutes which is typically enough time to complete the attack. Because its buffer is full, this port on the computer at the source address no longer responds to communication initiation messages.

A sync message is then generated and transmitted to the computer at the destination address which now defines the target computer (Block 114). The process waits for a sync/ack message from the computer at the destination address (Block 116). When it is received, the process retrieves the TCP sequence number from the TCP segment header (Block 120) and checks to see if a predetermined number of TCP sequence numbers have been retrieved from the target computer at the destination address (Block 122). If the predetermined number of sequence numbers has not been received, a time period corresponding to the unit of time between changes in TCP sequence number modifications is delayed. This delay permits the computer at the destination address to modify the TCP sequence number which is used for initiating a communication session. Alternatively, the destination port address on the target computer may be changed to cause a sequence number increment as well. After this delay has expired or the destination port address changed, another sync message is generated and sent to the target computer (Block 114). When the predetermined number of TCP sequence numbers have been received, the TCP numbers are used to evaluate the offset between TCP sequence numbers or the pattern for generating the TCP numbers (Block 126). For example, if a predetermined offset amount is added to generate a new TCP sequence number for communication initiation, three TCP sequence numbers may be used to compute the difference between two adjacent TCP numbers. This difference should indicate the predetermined offset so that the next TCP sequence number which would be used by the target computer to respond to a new sync message is determined.

The IP spoofing attack process continues by setting the source address in the network layer 24 to the source address retrieved from source/destination address generator 34 (Block 130). Now messages generated by the computer implementing the system and method of the present invention generates messages which appear to be originated from the computer at the source address. A communication initiation message is then generated and transmitted to the computer at the destination address (Block 132). A period of time is delayed which corresponds to the normal response time for the target computer to send a sync/ack message. The process then prepares an ack message with the predicted TCP sequence number (Block 134). A service command is obtained from a service command generator 36 and placed in a TCP segment passed to transport layer 22 to build a service command message (Block 138). Both messages are then transmitted to the target computer to emulate an ack message and service command message from the emulated computer with the blocked port. If the predicted TCP sequence number for the ack message having the source address of the emulated computer matches the TCP sequence number sent by the target computer in the sync/ack message, the target computer establishes a communication connection which accepts messages having a source address of the emulated computer. Now the service command message sent from the computer implementing the process of FIG. 3 is accepted and executed by the service coupled to the port if the command is valid for the service. Preferably, the service command causes the computer at the destination address to log the attack at the computer which has been compromised and, most preferably, the command causes the target computer to send a compromise indicator to the computer implementing the process of FIG. 3, although another computer may receive the compromise indicator. The success or failure of the attack is logged (Block 142–146). Preferably, a Telnet session is established between the compromised target computer and the computer executing the program which implements the process of FIG. 3. Initiation of the Telnet session may be logged to record the success of the IP spoofing attack and additional information may be obtained during the Telnet session about the compromised computer to search for other security vulnerabilities of the target system.

The process then determines whether another source address exists on the network (Block 148), and if there is, an attack on the target computer is attempted using the computer at the new source address as the emulated computer. If all of the source addresses have been used, the process checks to see if another destination address is available (Block 150). If another source address is available, the process is repeated to evaluate attacks from each of the other computers on the network on the target computer defined by the new destination address. This process continues until each computer on the network has been used to attack all the other computers on the network. Once this has been done, the attack log may be stored in table 46. The log may be later displayed to identify those computers on the network that are susceptible to IP spoofing attacks or provide other information obtained from the target computers that were compromised (Block 152).

Another embodiment of the present invention is shown in FIG. 4. System 40 includes a communication initiation message generator 42 and a response message evaluator 44 for determining whether a service is coupled to a port responding to a communication initiation message. System 40 builds a topology table 46 of service ports for network 12 from the communication initiation responses without causing a communication connection which may be logged by the computer having the ports which are being interrogated. Communication initiation message generator 42 is coupled to transport layer 22 of protocol stack 20 so communication initiation messages may be provided to transport layer 22 for transmission to the ports of the other computers coupled to network 12. Preferably, the communication initiation messages are sync messages used in the three handshake protocol of a TCP/IP network. Response evaluator 44 is also coupled to transport layer 22 to receive the response messages to the communication initiation messages sent by a computer executing a program implementing the process shown in FIG. 5. If the response message is the handshake acknowledgment message in the communication connection process, response evaluator 44 records the port address as a service access port for network 12 in table 46. In the three handshake protocol used to establish a communication connection on a TCP/IP network, a sync/ack message is the handshake acknowledgment message which indicates a service is present on a port.

The process implemented by system 40 of FIG. 4 is shown in FIG. 5. The process begins with communication initiation message generator 42 obtaining a destination address of a computer on network 12 from source/destination address generator 34 (Block 200) and the destination port address is set to the first port address on the destination computer (Block 202). Most computers in a TCP/IP protocol have port addresses in the range of 0–65,535. Preferably, each port address is tested by system 40. A communication initiation message is generated for the first port address of the computer at the destination address and passed to transport layer 22 (Block 206). After the communication initiation message is transmitted, response evaluator 44 waits for receipt of a response message from the port to which the communication initiation message was sent (Block 210). Response evaluator 44 then determines whether the message is a handshake acknowledgment message (Block 212). If it is, response evaluator 44 stores a service indicator, the destination address and port address in service topology table (Block 216). In a TCP/IP network, a sync/ack message indicates a service is coupled to the port while a reset message indicates no service is coupled to the port. The process then checks to see if the port address is the last possible port address on the computer (Block 218). If it is not, the port address is incremented (Block 220) and a new communication initiation message is sent to the next port address of the computer at the destination address (Block 206). The process continues until all of the port addresses on a computer have been tested to determine whether a service is coupled to each port. After each port has been checked for a service, the process determines whether another destination address is available (Block 224). If there is, another destination address is obtained (Block 200) and the process continues at the first port address for the next computer. The process terminates when all of the computers on network 12 have been checked.

Another embodiment of the present invention is shown in FIG. 6. In system 50, a RPC message generator 52 and response evaluator 54 are coupled to transport layer 22. RPC message generator 52 generates a data segment having a command for an RPC service which may not require an authorization check such as a password. Response message evaluator 54 determines from a message received in response to the RPC service command message whether an RPC service having little or no authorization check is available over the network. A record of this service may be provided to the system or network administrator.

The process implemented by system 50 is depicted in FIG. 7. The process begins by obtaining a destination address for a computer on the network 12 from source/destination address generator 34 (Block 240). The destination port address is initialized to the first port address on the computer at the destination address (Block 242) and a first RPC service command is generated by RPC message generator 52 (Block 244). Preferably, a CONNECT command which identifies the destination address and port address is issued to transport layer 22 (Block 248). Once a communication connection has been established, transport layer 22 notifies RPC message generator 52 (Block 250). RPC message generator 52 then passes the generated service command to transport layer 22 and a message containing the service command is transmitted to the port with which communication has been established (Block 252). Response message evaluator 54 then waits for a response (Block 254). If a response is detected which indicates the service command was executed (Block 258), the destination address, port address and type of RPC service is stored in topology table 46 (Block 260). If no communication connection was established with the port, no entry is made for the port. If communication is established but the port does not respond to the first service command, RPC message generator 52 determines if another RPC service command is available (Block 262) and, if there is, it generates a service command for another service (Block 264) and passes the command to transport layer 22 (Block 252). There are a number of known RPC commands for the UNIX operating system and RPC message generator 52 may generate a service command for each one to determine if it exists on a port being tested. If the process does not determine that an RPC service is coupled to the port, it identifies the service as a non-RPC service and stores an unknown or non-RPC service indicator in table 46 (Block 266). Response evaluator 54 evaluates any message received which was responsive to the next service command (Blocks 254, 258). After the process finishes its interrogation of a port for the type of service coupled to the port, the process determines whether another port exists (Block 270). If there are other ports to be interrogated, the port address is incremented (Block 272) and the process continues until all the ports on the computer at the destination address have been tested. The process then continues by determining whether another destination address for a computer on the network exists (Block 276) and, if it does, repeating the process for each port on that computer. When the process of FIG. 7 is completed, a topology map has been built which identifies the port and the RPC service coupled to each port for each computer on the network.

System 50 of FIG. 6 may be combined with system 40 of FIG. 4 such that once topology table 46 identifying those ports which are coupled to a service has been generated by response evaluator 44 of system 40, RPC message generator 52 need only attempt to identify which of the ports identified as being coupled to a service are coupled to an RPC service having little or no authorization check. Response evaluator 54 of system 50 message generator may then identify the RPC services for those ports which respond to service commands generated by RPC message generator 52.

An embodiment used to test the configuration of a router is shown in FIG. 8. System 60 includes a communication message generator 62 and a response evaluator 64. Preferably, communication message generator 62 includes a source routing verifier 66, a source porting verifier 68 and a Socks configuration verifier 70. Socks configuration verifier 70 and source routing verifier 66 execute in the application layer of a computer which is located outside network 12 and router RI which controls access to network 12. Source porting verifier 68 specifies a source port for data messages being sent to a computer on network 12 and, consequently, it communicates with transport layer 22 and network layer 24 of protocol stack 20 on the computer executing the program which implements system 60.

The process performed by the source routing verifier 66 is shown in FIG. 9. That process begins by obtaining a destination address for a computer on network 12 from source/destination address generator 34 (Block 300). The computer to which the message is to be ultimately delivered is defined by a destination address. The source address used to identify an intermediate source for a source routed message is also obtained from source/destination address generator 34 (Block 302). Source routing verifier 66 then passes the source and destination addresses to transport layer 22 (Block 306) to source route a message to a computer at the destination address on network 12 through the intermediate source identified by the source address (Block 310). If a response is detected by response message evaluator 64 to the source routed message (Block 312), a log indicating that the source routing blocking feature is not activated for the particular source/destination address combination is recorded in table 46 (Block 314). If another source address is available for another computer on the network (Block 316), it is obtained and another source routed message through the selected source address to the destination address is attempted. After attempts to source route messages to the destination address through all the source addresses for the other computers on the network have been attempted, the process determines if all destination addresses have been tested (Block 318). If another destination address is available, another destination address is obtained and the process is repeated using the addresses of the other computers on the network as source addresses for source routed messages to the next destination address. In this manner, a log of all the source routed combinations which are not being blocked by the router are recorded in table 46 so the router may be reconfigured.

FIG. 10 shows a process implemented by source porting verifier 68. The process begins by obtaining a destination address for a computer on the network from source/destination address generator 76 (Block 340). Preferably, a source port address which corresponds to the default FTP source port address, typically port address 20, is provided to network layer 24 (Block 342). Until it is changed, data messages from the computer executing the program which implements the process of FIG. 11 generates data messages having a source port address of 20. The destination port address is set to the first port address (Block 344) and a data message having a source port address of 20 is sent to the port of the computer at the destination address (BLOCK 348). Response evaluator 72 evaluates the responsive message received (Block 350), if any, to determine whether the port responded to the source ported data message. Each response is stored in table 46 (Block 354). The process determines if there is another destination port address (Block 358) and, if there is, the destination port address is incremented (Block 360). The process continues by checking the next destination port. If all the destination ports on the destination computer have been checked, the process determines if another source port address is to be tested (Block 364). If there is, the next source port address is obtained (Block 366) and the ports of the destination computer are tested with messages having the new source port address. Alternatively, all source port addresses may be exhaustively tested. If there are no more source port addresses to check, the process determines if another destination address exists on the network (Block 368). If it does, the next destination address is obtained (Block 340) and the process continues. Otherwise, the process stops.

A router may be configured with a rule which blocks data messages from computers external to network 12. However, another rule may permit messages with certain source port address values to pass through in order to support certain services such as FTP. FTP requires a source port address of 20. A hacker may attempt to get into a network by sending messages with a source port value which a router passes because it conforms to the rule for FTP messages. The process of FIG. 10 determines whether messages with predetermined source port addresses from computers external to the network are able to be received by computers on a network despite router configuration rules which would otherwise prevent the transmission of the messages.

As discussed above, Socks servers do not pass simply pass messages between computers on the network and those external to the network but instead require two separate communication connections. One communication connection is with an external computer and the other communication connection is with a computer on the network. In this manner, the Socks server may more thoroughly examine message in accordance with the rules configured for the server before passing the messages from one communication connection to another communication connection.

A preferred process implemented by the Socks configuration verifier of FIG. 8 is shown in FIG. 11. That process begins by having the computer executing the program which implements the process of FIG. 11 connect to the Socks server (Block 400). A destination address is then obtained from the source/destination address generator 34 and used to request that the Socks server connect to the computer on the network at the destination address (Block 402). The destination port address is set to the first port address value of the possible range of port address values (Block 406). A service command is then generated (Block 410) and a service command message addressed for the computer at the destination address is sent to the Socks server (Block 412). The process then waits for a response (Block 416). The response message is evaluated by response message generator 64 to determine if the response message indicates that the computer at the destination address received the service command (Block 420). If it did not, the process determines if another communication method is available (Block 424). If there is, the service command message is modified for another communication method (Block 426) and sent to the Socks server (Block 412). For example, if the message did not go through the Socks server, the service command message may be reformatted as a source routed message or a message with a predetermined source port value to see if the Socks server passes that type of message to the computer at the destination address. If no other communication format is available, the process continues by determining if another port address is available (Block 438).

If the message indicates that the computer on the network responded to the service command, the process determines whether the service command was executed (Block 430). If it was, the service and port address are stored in table 46 (Block 432). If the response message indicates that the service command was received but not executed, the process determines if another service command is available (Block 434). If there is, a new service command is generated (Block 410) and the process continues until all service commands have been attempted for the port address at the destination address computer. If no other service commands remain to be tried, an indicator is stored in table 46 which indicates communication was established with the port address but no service was executed (Block 432).

The process continues by determining if another port address remains for the computer at the destination address (Block 438). If one does, the port address is incremented (Block 440) and the testing for the new port address continues (Block 410). Otherwise, the process determines whether another destination address is available on the network (Block 444). If there is, it is obtained from source/destination address generator 34 (Block 402) and testing of the computer at the new destination address continues. Otherwise, the communication connection with the Socks server is terminated and the process stops.

A more preferred embodiment of the present invention is shown in FIG. 12. System 80 includes IP spoofing attack generator 32, communication initiation message generator 42, RPC message generator 52, communication message generator 62, source/destination address generator 34, topology table or log 46 and protocol stack 20 which operate in manner consistent with the description of the embodiments for those like numbered components discussed above. System 80 also includes response evaluator 82 which includes the functionality of response message evaluators 44, 54 and 64 as discussed above. A Graphic User Interface (GUI) 84 is also provided to accept input and control from a user and to display options and information to a user in a known manner. A user may use GUI 84 to activate each of the network verifiers 32, 42, 52 or 62 individually or selectively identify a group of verifiers to automatically execute and build the information in table 46. GUI 84 also permits a user to enter information for execution of the verifiers such as defining or adding predetermined source port addresses, RPC services, addresses for computers added or deleted from a network or the like.

In operation, a user activates the program which implements an embodiment of the present invention such as system 80. As a result, GUI 84 may present options to the user such as modifying information for system operation, selection of one or more of the network verifiers or display of stored information. After the user makes a selection, system 80 then performs the requested option. For example, if the user selects the system information modification option, the user is permitted to change system information such as adding addresses for new computers on a network. GUI 84 then returns the user to the main option menu following completion of the input of data and the user may now select one or more network verifiers to run. GUI 84 then selectively activates the selected network verifiers which communicate with protocol stack 20 to communicate messages between the computer executing system 80 and a computer on the network being tested or a router or a Socks server coupled to the network. When the verification tests or scans are completed, the user may select the display option and either view or print the information The user may then use the displayed information to add authorization checks to services or new rules to a Socks server or router.

While the present invention has been illustrated by the description of a number of embodiments and while the embodiments have been described in considerable detail, it is not the intention of the applicant to restrict or any way limit the scope of the appended claims to such detail. Additional advantages and modifications will readily appear to those skilled in the art. The invention in its broader aspects is therefore not limited to the specific details, representative systems and methods, and illustrative examples shown and described. Accordingly, departures may be made from such details without departing from the spirit or scope of applicant's general inventive concept.

What is claimed is:

1. A system for detecting a security vulnerability in open network communications comprising:

an internet protocol (IP) spoofing attack generator for generating an IP spoofing attack on a target computer coupled to an open network to determine whether said target computer is vulnerable to an IP spoofing attack which emulates communication from another computer on said open network;

a service command message generator for generating a service command to be executed by a service coupled to a port on said target computer; and

said IP spoofing attack generator transmitting said service command to said target computer to generate a response in said target computer that provides a compromise indication without altering system operational parameters of said target computer.

2. The system of claim 1, wherein said generated service command is for one of an rsh and an rlogin service to determine whether authorization checks for said service exist.

3. The system of claim 2, wherein said generated service command causes said target computer to generate an electronic mail message indicative that said target computer has been compromised.

4. The system of claim 3, wherein said generated service command causes said target computer to initiate a Telnet

session with a computer which logs said Telnet session to indicate said target computer has been compromised.

5. The system of claim 1, further comprising:

a source/destination address generator which generates source and destination addresses for messages corresponding to an open network protocol used to communicate on said open network, said destination address corresponding to said target computer and said source address corresponding to said computer being emulated for said attack.

6. The system of claim 5, wherein said source/destination address generator generates source and destination address combinations which are used by said IP spoofing attack generator to test vulnerability of each computer in said open network to an IP spoofing attack which emulates communication from each of said other computers on said open network.

7. A system for generating a service topology map for each computer on an open network without completing a communication connection with any computer on the open network comprising:

a communication initiation message generator for generating communication initiation messages, said communication initiation messages being transmitted to ports on a computer on an open network; and

a response message evaluator for determining from response messages received from said ports receiving said communication initiation messages whether services exist on said ports receiving said communication initiation messages, said response messages not completing communication connections with said ports so that services coupled to said ports may be detected without completing communication connection with said ports.

8. The system of claim 7, further comprising:

a table for storing service indicators indicative of which ports responding to said communication initiation messages are coupled to services.

9. The system of claim 8, wherein said communication initiation message generator generates a communication initiation message for each port address on a computer on said open network.

10. The system of claim 9, wherein a source/destination address generator generates a destination address for each computer on an open network so that each port on each computer on said open network receives a communication initiation message and said table contains service indicators for each port of each computer on said open network which responds to said communication initiation messages.

11. The system of claim 7, wherein said communication initiation message generator generates sync messages for a TCP/IP protocol.

12. The system of claim 11, wherein said response message evaluator determines a service is coupled to a port receiving a communication initiation message in response to detecting a sync/ack message.

13. The system of claim 7, wherein said communication initiation message is the first message for a three handshake protocol to establish a communication connection.

14. A system for detecting vulnerability of ports coupled to remote procedure call (RPC) services on a computer of an open network comprising:

a remote procedure call (RPC) message generator for generating and sending RPC service commands to ports on a computer on an open network; and

a response message evaluator for evaluating response messages from said ports of said computer receiving said RPC service commands, said response messages indicating whether said RPC service commands were executed by an RPC service coupled to said ports of said computer receiving said RPC service commands without establishing a communication connection with said ports.

15. The system of claim 14, further comprising:

a table for storing port addresses and service indicators that indicate which particular RPC services are coupled to ports receiving said service commands.

16. A system for detecting vulnerabilities in routers comprising:

a communication message generator for generating and sending service commands from a computer external to an open network to ports on computers coupled to said open network through a router; and

a response message evaluator for evaluating response messages received from said ports on computers of said open network in response to said service commands sent from said communication message generator external to said open network whereby access to said computers on said open network through said router may be determined without referencing configuration files of said router.

17. The system of claim 16, wherein said communication message generator includes a source routing verifier for generating source routed messages with a destination address of a computer on said open network and an intermediate source address on said open network; and

said response message evaluator evaluating response messages received from said ports on computers of said open network in response to said service commands sent from said communication message generator external to said open network to detect a vulnerability in said router of permitting source routed messages to bypass rules configured for filtering inbound messages on said router.

18. The system of claim 17, wherein each source address for each computer on said open network is used as said intermediate source address with each destination address for each computer on said open network to test each possible intermediate source/destination address combination for source routed messages on said open network.

19. The system of claim 18, further comprising:

a table for storing indicators for each intermediate source address/destination address combination that is detected as being vulnerable to receiving source routed messages.

20. The system of claim 16, wherein said communication message generator includes a source porting verifier for generating service command messages with a source port address having a predetermined value; and

said response message evaluator evaluating response messages received from said ports on computers of said open network in response to said service command messages having said predetermined source port address values sent from said source porting verifier external to said open network to detect said router passing messages having said predetermined source port address values to ports coupled to services on said open network.

21. The system of claim 20, wherein service command messages having said predetermined source port address value are sent to each computer on said open network.

22. The system of claim 21, further comprising:

a table for storing service indicators for each computer address that is detected as being vulnerable to receiving source ported messages.

23. The system of claim 22, wherein said predetermined value corresponds to a default source port address for a file transfer protocol (FTP) message of a TCP/IP protocol.

24. The system of claim 16, further comprising:

a Socks configuration verifier for establishing a communication connection with a Socks server and for sending service command messages to computers on said open network coupled to said Socks server; and

said response message evaluator evaluating said messages received in response to said service command messages to determine whether said service command message was passed by said Socks server to one of said computers on said open network.

25. The system of claim 24 said response message evaluator determining whether said service command message was executed by said one computer on said open network.

26. The system of claim 25 said response message evaluator storing service indicators indicative of said services which executed said service command messages received at said port addresses.

27. A method for detecting a security vulnerability in an open network comprised of the steps of:

attempting an Internet Protocol (IP) spoofing attack against a target computer and open network;

generating a service command message; and

sending said service command message to said target computer following said IP spoofing attack to determine whether said target computer has been compromised, said service command message generating an indicator of the success of the IP spoofing attack without altering the operational parameters of the target computer.

28. The method of claim 27, wherein said generating service command message step generates one of an rsh and rlogin command.

29. The method of claim 28, wherein said generating step:

generates an electronic mail message indicative of the success of the IP spoofing attack in response to said service command message.

30. The method of claim 27, further comprising the step of:

initiating a Telnet session between said target computer and another computer to indicate the success of said IP spoofing attack in response to said service command message.

31. The method of claim 27, further comprising the steps of:

generating source addresses and destination addresses for said IP spoofing attack; and

attempting said IP spoofing attack against each said generated destination address by emulating communication from each of said source addresses.

32. A method for generating a service topology map of an open network comprising the steps of:

generating a communication command initiation message;

sending said communication command initiation message to a port on a computer on an open network;

receiving a message from said port in response to said communication initiation message being received at said port; and

evaluating said message received from said port to determine whether a service is coupled to said port without establishing a communication connection with said port.

33. The method of claim 32, further comprising the step of:

storing a service indicator to provide a reference that said port has a service coupled thereto which may be accessed from another computer.

34. A method for detecting availability of a service on a port of a computer on an open network comprising the steps of:

generating a service command message;

sending said generated service command message to a port of a computer on said open network;

receiving a message from said port in response to said port receiving said generated service command message; and

evaluating said message received from said port to determine whether a service coupled to said port executed said service command message, without establishing a communication connection with said ports.

35. The method of claim 34, further comprising the step of:

storing a service indicator indicative that said service coupled to said port executed said service command message.

36. The method of claim 35, wherein said generating step generates service command messages for different services; and

said evaluating step determines the type of service coupled to said port which executed said service command message.

37. The method of claim 36, wherein said generating step generates said service command messages for each port of a computer of said open network.

38. The method of claim 34, further comprising the steps of:

establishing a communication connection with a Socks server;

requesting said Socks server establish a communication connection with a computer on said open network; and

said evaluating step determining whether said Socks server is configured to stop said service command message from being sent to said port of said computer of said open network.

39. The method of claim 34, wherein said generating step generates remote procedure call (RPC) service command messages.

40. The method of claim 34, wherein said generating step generates service command messages having predetermined source port addresses.

41. The method of claim 34, wherein said generating step generates source routed service command messages.

* * * * *

US005805801A

United States Patent [19]

Holloway et al.

[11] **Patent Number: 5,805,801**

[45] **Date of Patent: Sep. 8, 1998**

[54] **SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY**

[75] Inventors: **Malcolm H. Holloway**, Durham; **Thomas Joseph Prorock**, Raleigh, both of N.C.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **780,804**

[22] Filed: **Jan. 9, 1997**

[51] **Int. Cl.**[6] **G06F 11/00**

[52] **U.S. Cl.** **395/187.01**

[58] **Field of Search** 395/186, 187.01, 395/182.02, 200.55; 380/3, 25; 370/434, 488

[56] **References Cited**

U.S. PATENT DOCUMENTS

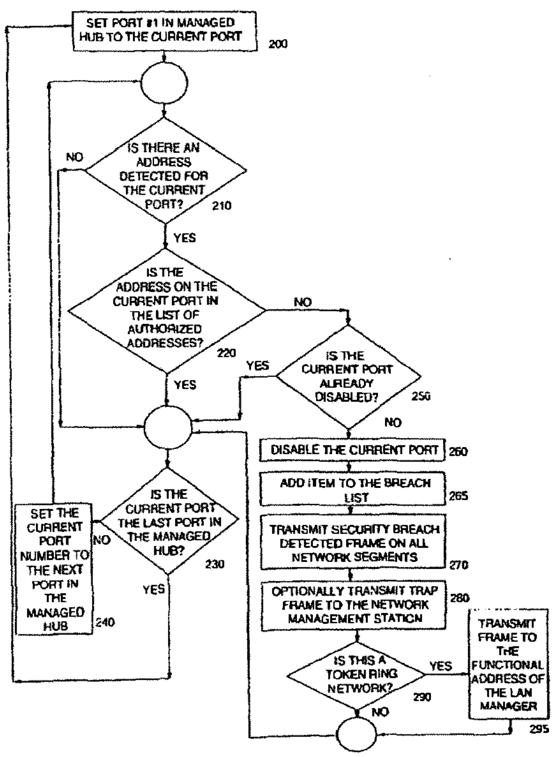
4,930,159	5/1990	Kravitz et al.	380/23
5,177,788	1/1993	Schanning et al.	380/23
5,305,385	4/1994	Schanning et al.	380/45
5,311,593	5/1994	Carmi	380/23
5,337,309	8/1994	Faulk, Jr.	
5,414,833	5/1995	Hershey et al.	380/4
5,440,723	8/1995	Arnold et al.	395/181
5,537,099	7/1996	Liang	340/825.07
5,606,668	2/1997	Shwed	395/200.11
5,610,981	3/1997	Mooney et al.	380/25
5,727,146	3/1998	Savoldi et al.	395/187.01

Primary Examiner—Albert Decady
Attorney, Agent, or Firm—John J. Timar

[57] **ABSTRACT**

A system and method for providing security against intrusion in a campus LAN network is provided. A managed hub discovers each interconnect device in the network that supports the security feature and maintains an interconnect device list of such devices, which may include token ring switches, Ethernet switches, bridges and routers. The managed hub detects an intrusion by an unauthorized address on one of its ports and notifies the interconnect devices of the intrusion by transmitting a security breach detected frame. The interconnect devices set a filter on their respective ports against the intruding unauthorized address. The interconnect devices send a filter set frame to the managed hub which reenables the port where the security intrusion occurred, after all filter set frames are received. A network management station sends a security clear condition frame to remove the filters.

59 Claims, 16 Drawing Sheets



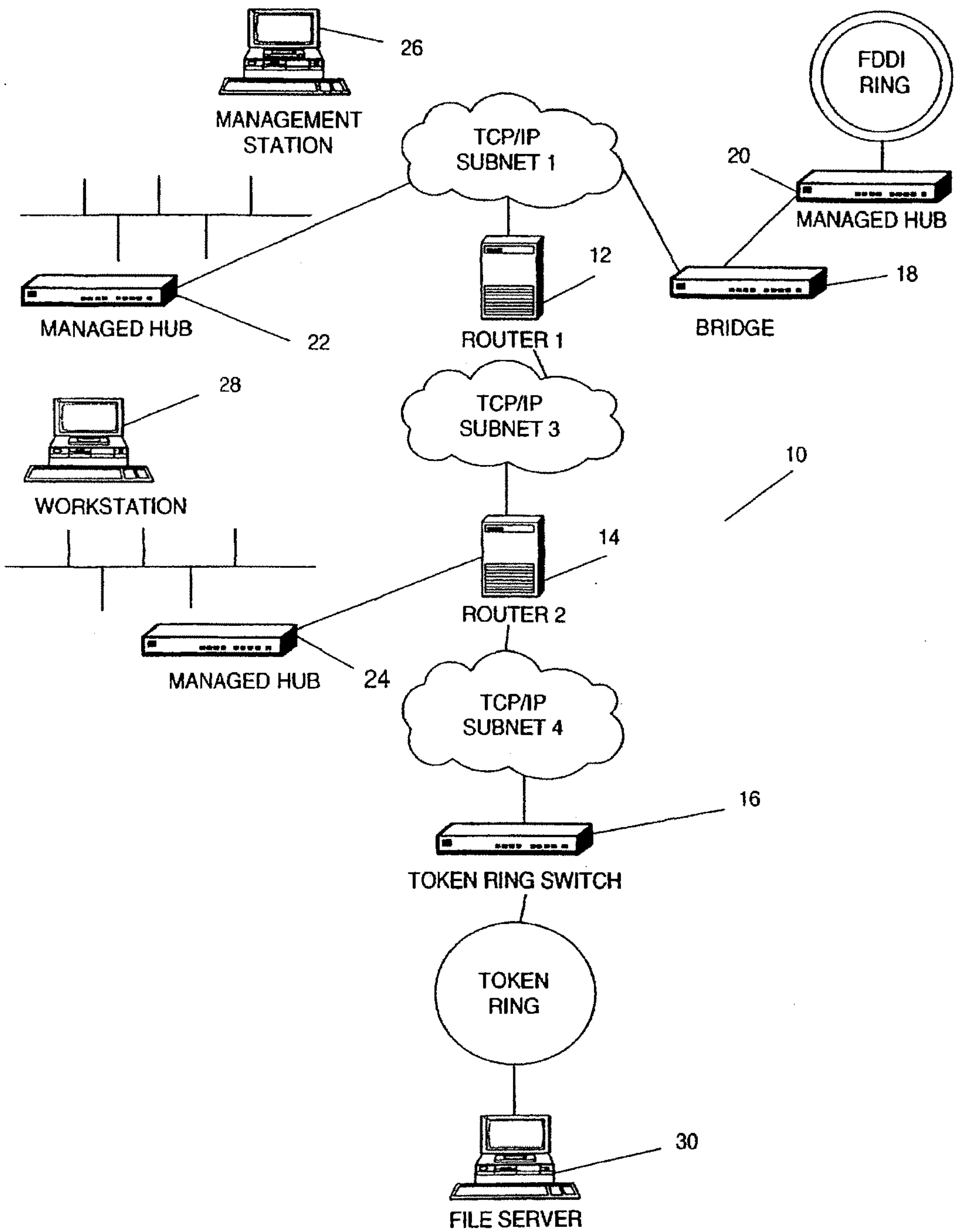

26
MANAGEMENT STATION
TCP/IP SUBNET 1
FDDI RING
20
MANAGED HUB
12
18
MANAGED HUB
22
ROUTER 1
BRIDGE
28
TCP/IP SUBNET 3
WORKSTATION
10
14
ROUTER 2
MANAGED HUB
24
TCP/IP SUBNET 4
16
TOKEN RING SWITCH
TOKEN RING
30
FILE SERVER

FIG. 1

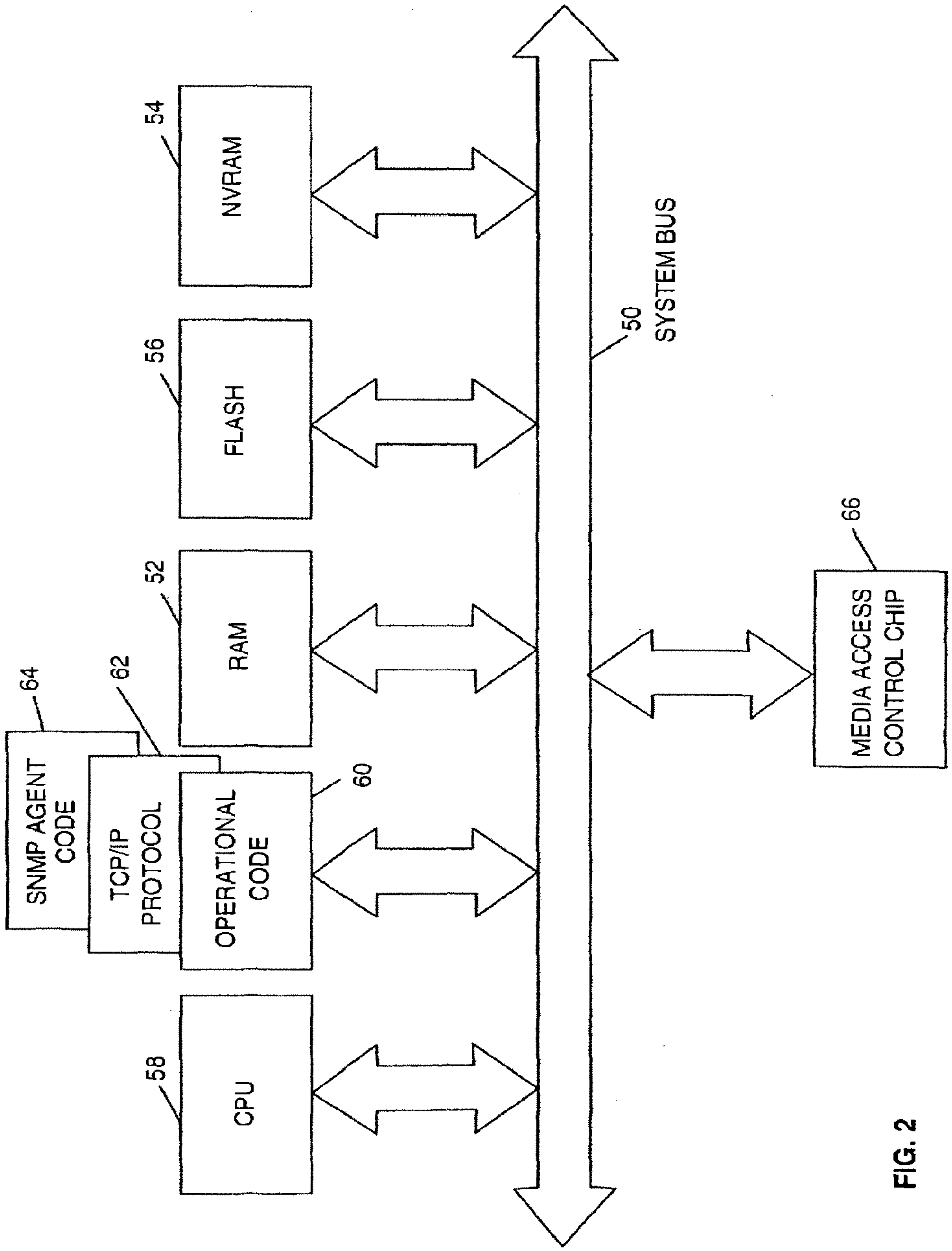

54
NVRAM
56
FLASH
52
RAM
64
SNMP AGENT CODE
62
TCP/IP PROTOCOL
60
OPERATIONAL CODE
58
CPU
50
SYSTEM BUS
66
MEDIA ACCESS CONTROL CHIP

FIG. 2

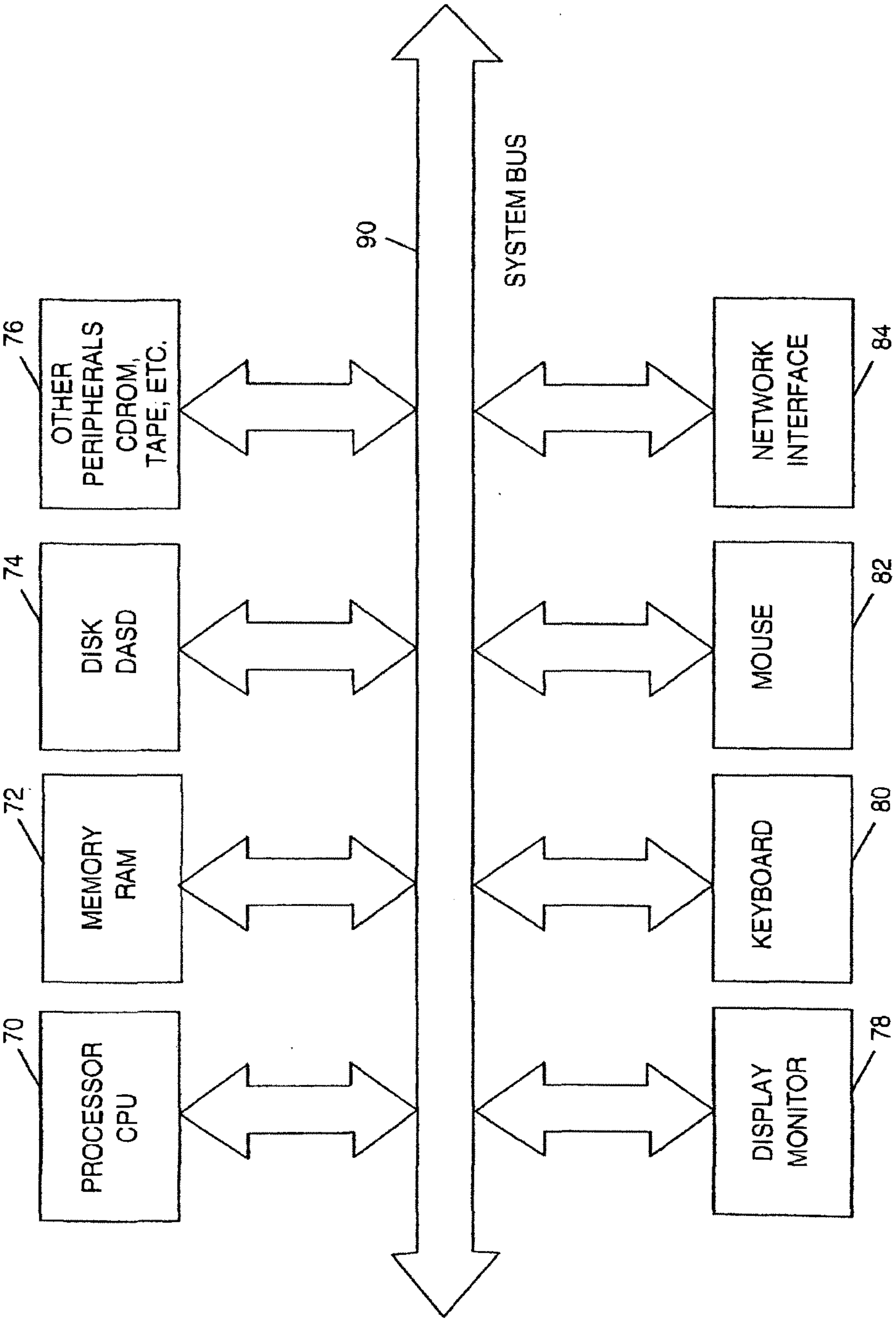

90
SYSTEM BUS
70
PROCESSOR CPU
72
MEMORY RAM
74
DISK DASD
76
OTHER PERIPHERALS CDROM, TAPE, ETC.
78
DISPLAY MONITOR
80
KEYBOARD
82
MOUSE
84
NETWORK INTERFACE

FIG. 3

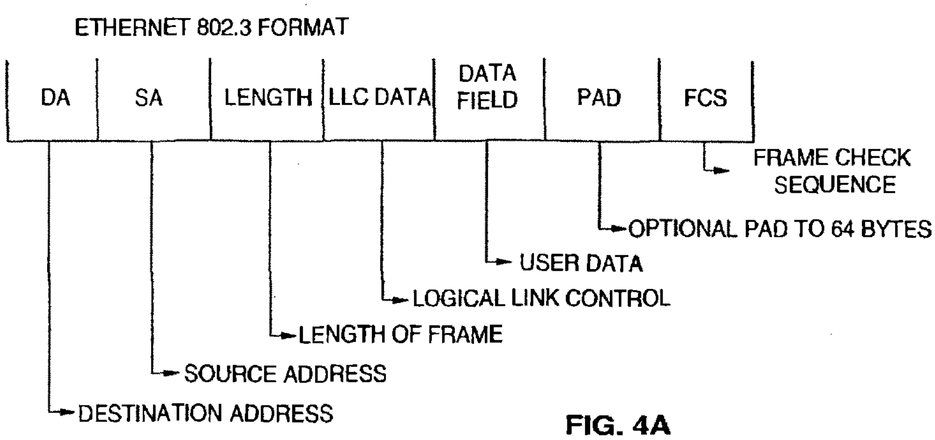


FIG. 4A

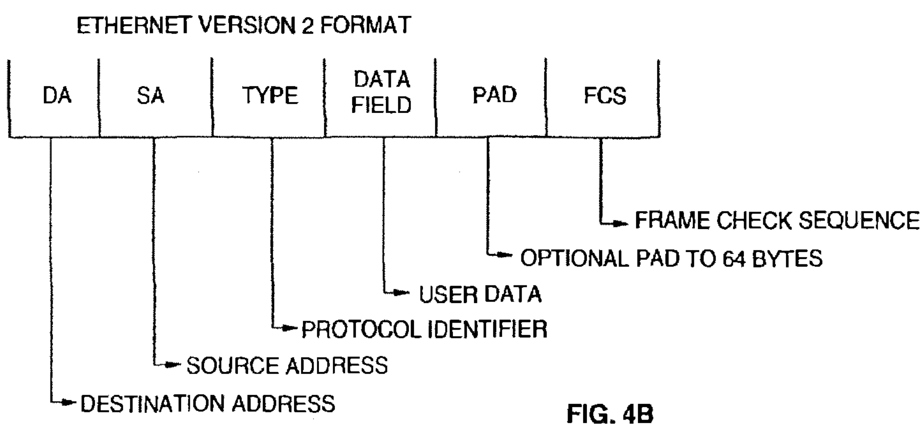


FIG. 4B

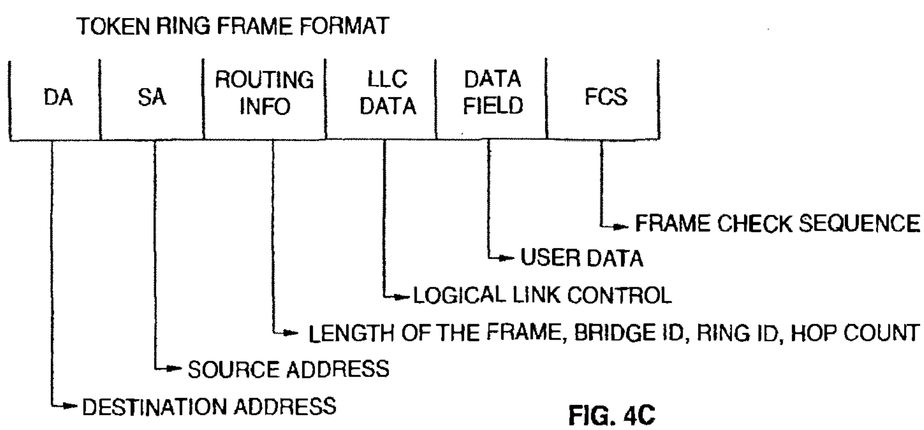


FIG. 4C

DISCOVERY REQUEST

FRAME TYPE IDENTIFIER	TIME STAMP	
1	4	BYTES

FIG. 5A

DISCOVERY RESPONSE

FRAME TYPE IDENTIFIER	INTERCONNECT DEVICE MAC ADDRESS	INTERCONNECT DEVICE DESCRIPTION	TIME STAMP	
1	6	50	4	BYTES

FIG. 5B

SECURITY BREACH DETECTED FRAME

	FRAME TYPE IDENTIFIER	INTRUDING MAC ADDRESS	MODULE NUMBER	PORT NUMBER	TIME STAMP	DEVICE FIELD LENGTH	ADDRESSES
BYTES	1	6	1	1	4	2	VARIABLE LENGTH

FIG. 5C

FILTER SET FRAME

FRAME TYPE IDENTIFIER	INTERCONNECT DEVICE MAC ADDRESS	INTRUDING MAC ADDRESS	MODULE NUMBER	PORT NUMBER	TIME STAMP	
1	6	6	1	1	4	BYTES

FIG. 5D

SECUITY CLEAR CONDITION

FRAME TYPE IDENTIFIER	INTRUDING MAC ADDRESS	
1	6	BYTES

FIG. 5E

INTERCONNECT DEVICE LIST ITEM			
MAC ADDRESS	DEVICE DESCRIPTION	LAST RESPONSE TIME	OUTSTANDING BREACH RESPONSE COUNT

MAC ADDRESS: MAC ADDRESS OF THE INTERCONNECT DEVICE
DEVICE DESCRIPTION: ASCII SELF DESCRIPTION PROVIDED BY THE INTERCONNECT DEVICE
LAST RESPONSE TIME: TIME WHEN LAST RESPONSE RECEIVED FROM INTERCONNECT DEVICE
OUTSTANDING BREACH RESPONSE COUNT: NUMBER OF SECURITY BREACH FRAMES THE INTERCONNECT DEVICE HAS NOT RESPONDED TO

FIG. 6

BREACH LIST ITEM				
MAC ADDRESS	BREACH TIME	BREACH PORT	BREACH MODULE	OUTSTANDING FILTER SET COUNT

MAC ADDRESS: MAC ADDRESS OF THE INTRUDING DEVICE
BREACH TIME: TIME WHEN INTRUSION OCCURED
BREACH PORT: PORT IN MANAGED HUB WHEN INTRUSION OCCURRED
BREACH MODULE: MODULE IN MANAGED HUB WHEN INTRUSION OCCURRED
OUTSTANDING FILTER SET COUNT: NUMBER OF FILTER SET FRAMES NOT RECEIVED YET

FIG. 7

INTRUSION LIST ITEM			
MAC ADDRESS	BREACH TIME	BREACH PORT	BREACH MODULE

MAC ADDRESS: MAC ADDRESS OF INTRUDING DEVICE
BREACH TIME: TIME WHEN INTRUSION OCCURRED
BREACH PORT: PORT IN MANAGED HUB WHEN INTRUSION OCCURRED
BREACH MODULE: MODULE IN MANAGED HUB WHEN INTRUSION OCCURRED

FIG. 8

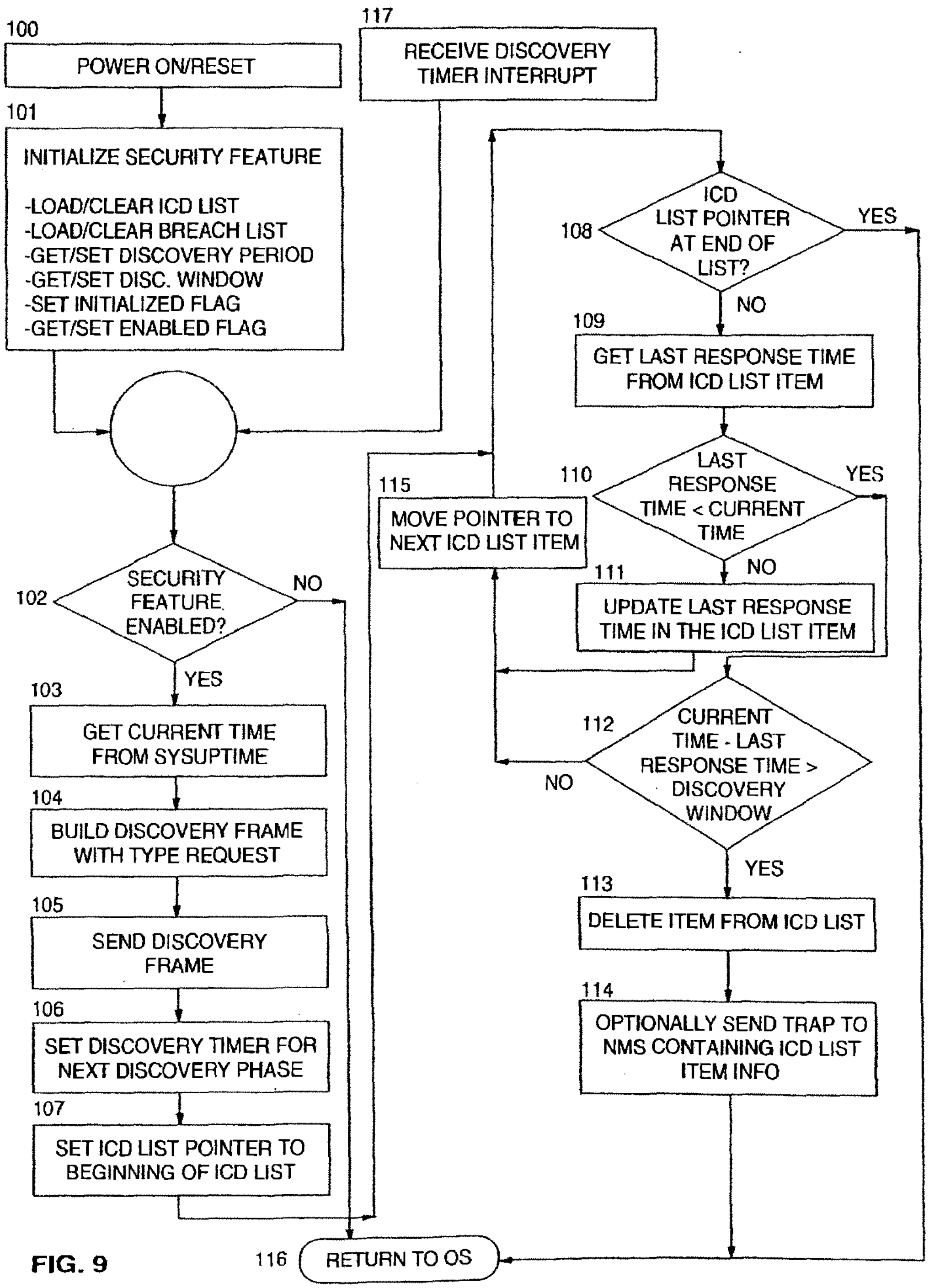

100
POWER ON/RESET
101
INITIALIZE SECURITY FEATURE
-LOAD/CLEAR ICD LIST
-LOAD/CLEAR BREACH LIST
-GET/SET DISCOVERY PERIOD
-GET/SET DISC. WINDOW
-SET INITIALIZED FLAG
-GET/SET ENABLED FLAG
117
RECEIVE DISCOVERY TIMER INTERRUPT
102
SECURITY FEATURE ENABLED?
NO
YES
103
GET CURRENT TIME FROM SYSUPTIME
104
BUILD DISCOVERY FRAME WITH TYPE REQUEST
105
SEND DISCOVERY FRAME
106
SET DISCOVERY TIMER FOR NEXT DISCOVERY PHASE
107
SET ICD LIST POINTER TO BEGINNING OF ICD LIST
108
ICD LIST POINTER AT END OF LIST?
YES
NO
109
GET LAST RESPONSE TIME FROM ICD LIST ITEM
110
LAST RESPONSE TIME < CURRENT TIME
YES
NO
115
MOVE POINTER TO NEXT ICD LIST ITEM
111
UPDATE LAST RESPONSE TIME IN THE ICD LIST ITEM
112
CURRENT TIME - LAST RESPONSE TIME > DISCOVERY WINDOW
NO
YES
113
DELETE ITEM FROM ICD LIST
114
OPTIONALLY SEND TRAP TO NMS CONTAINING ICD LIST ITEM INFO
116
RETURN TO OS

FIG. 9

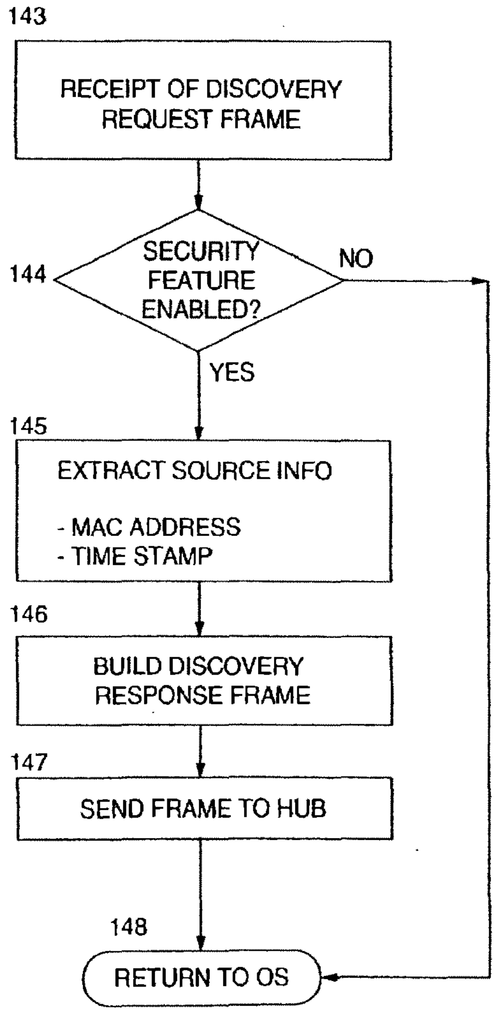

143
RECEIPT OF DISCOVERY REQUEST FRAME
144
SECURITY FEATURE ENABLED?
NO
YES
145
EXTRACT SOURCE INFO
- MAC ADDRESS
- TIME STAMP
146
BUILD DISCOVERY RESPONSE FRAME
147
SEND FRAME TO HUB
148
RETURN TO OS

FIG. 10

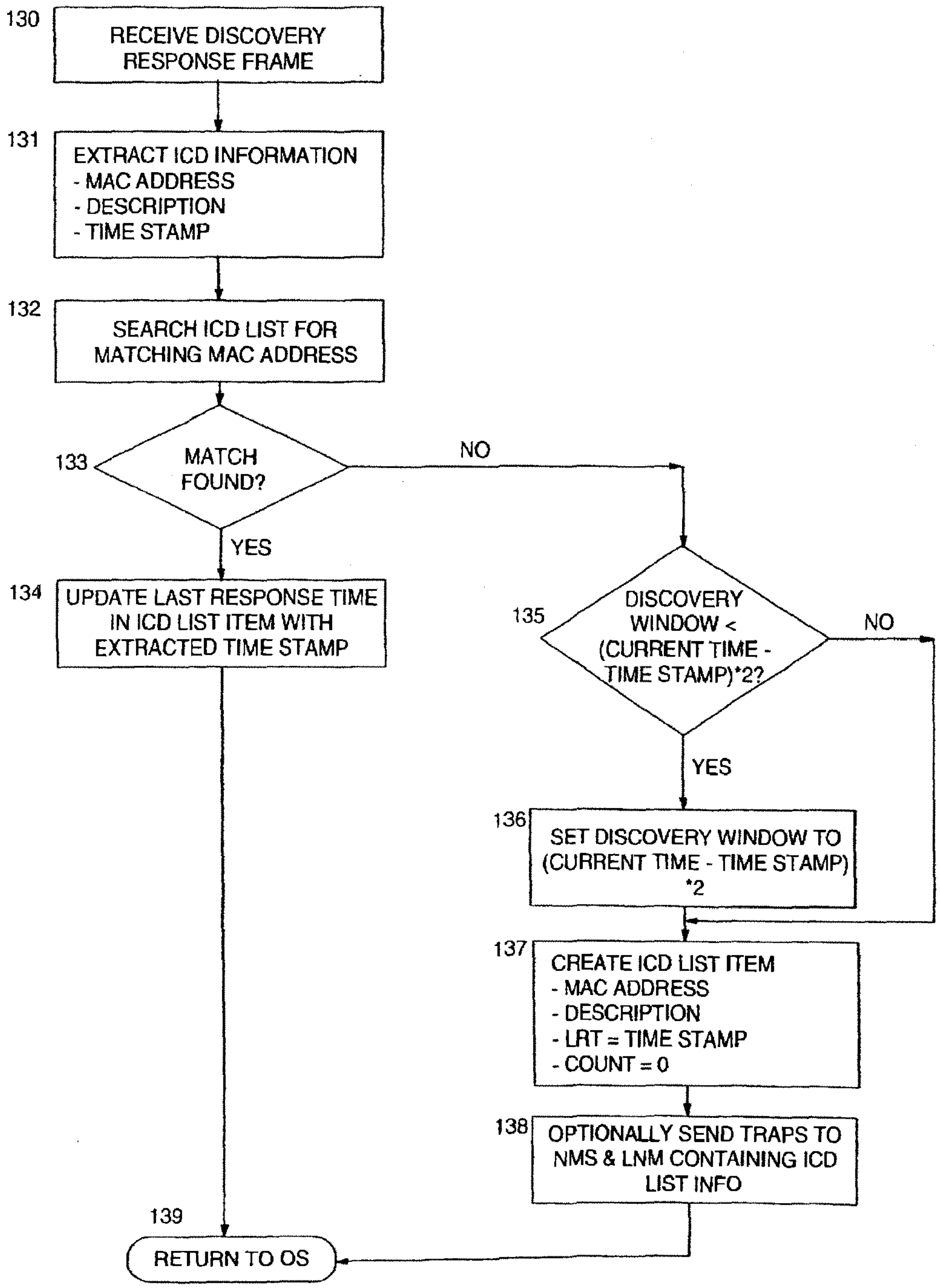

130
RECEIVE DISCOVERY RESPONSE FRAME
131
EXTRACT ICD INFORMATION
- MAC ADDRESS
- DESCRIPTION
- TIME STAMP
132
SEARCH ICD LIST FOR MATCHING MAC ADDRESS
133
MATCH FOUND?
NO
YES
134
UPDATE LAST RESPONSE TIME IN ICD LIST ITEM WITH EXTRACTED TIME STAMP
135
DISCOVERY WINDOW < (CURRENT TIME - TIME STAMP)*2?
NO
YES
136
SET DISCOVERY WINDOW TO (CURRENT TIME - TIME STAMP) *2
137
CREATE ICD LIST ITEM
- MAC ADDRESS
- DESCRIPTION
- LRT = TIME STAMP
- COUNT = 0
138
OPTIONALLY SEND TRAPS TO NMS & LNM CONTAINING ICD LIST INFO
139
RETURN TO OS

FIG. 11

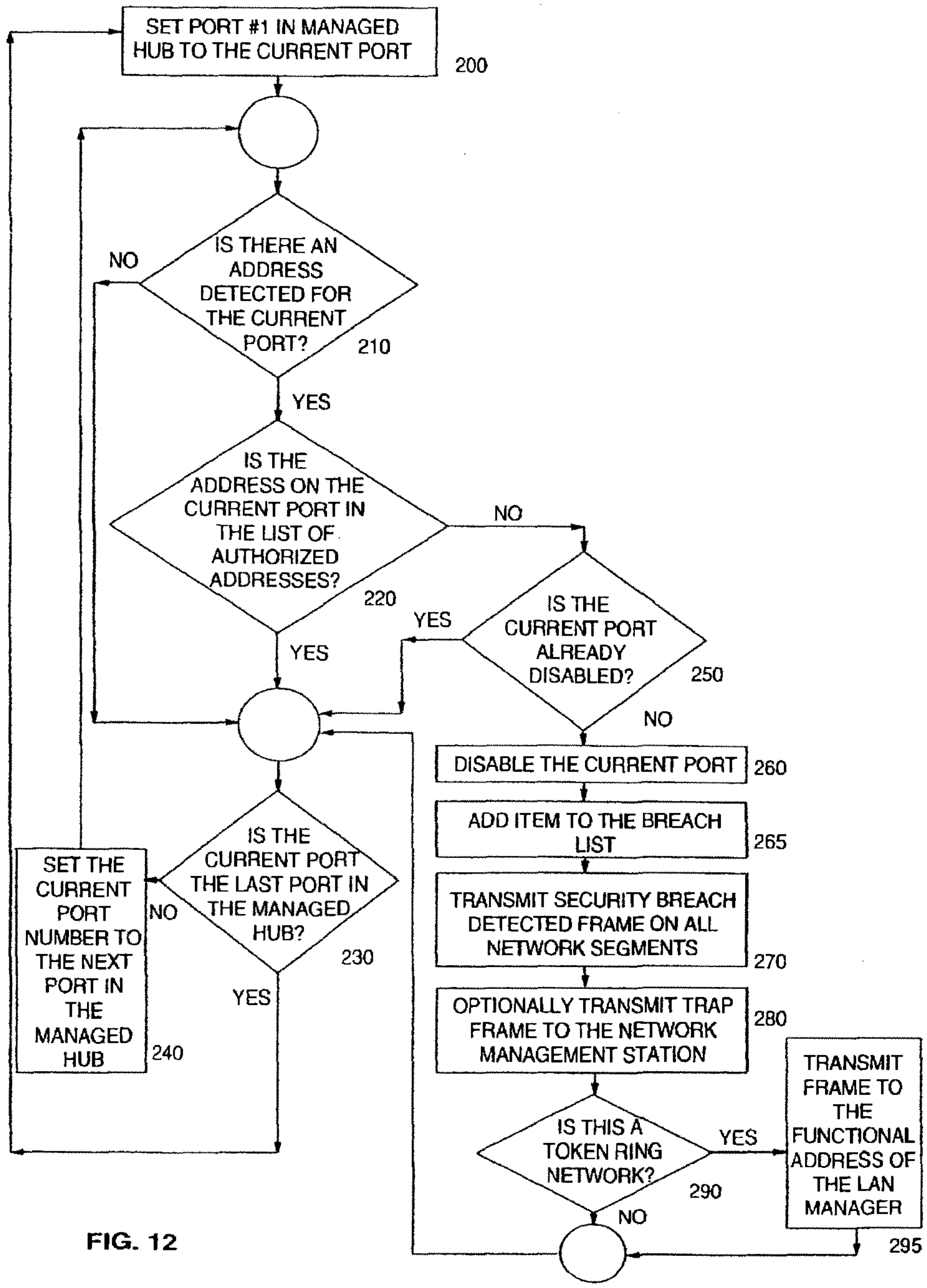

SET PORT #1 IN MANAGED HUB TO THE CURRENT PORT
200
IS THERE AN ADDRESS DETECTED FOR THE CURRENT PORT?
210
NO
YES
IS THE ADDRESS ON THE CURRENT PORT IN THE LIST OF AUTHORIZED ADDRESSES?
220
NO
YES
IS THE CURRENT PORT ALREADY DISABLED?
250
YES
NO
DISABLE THE CURRENT PORT
260
ADD ITEM TO THE BREACH LIST
265
TRANSMIT SECURITY BREACH DETECTED FRAME ON ALL NETWORK SEGMENTS
270
OPTIONALLY TRANSMIT TRAP FRAME TO THE NETWORK MANAGEMENT STATION
280
IS THIS A TOKEN RING NETWORK?
290
YES
NO
TRANSMIT FRAME TO THE FUNCTIONAL ADDRESS OF THE LAN MANAGER
295
IS THE CURRENT PORT THE LAST PORT IN THE MANAGED HUB?
230
NO
YES
SET THE CURRENT PORT NUMBER TO THE NEXT PORT IN THE MANAGED HUB
240

FIG. 12

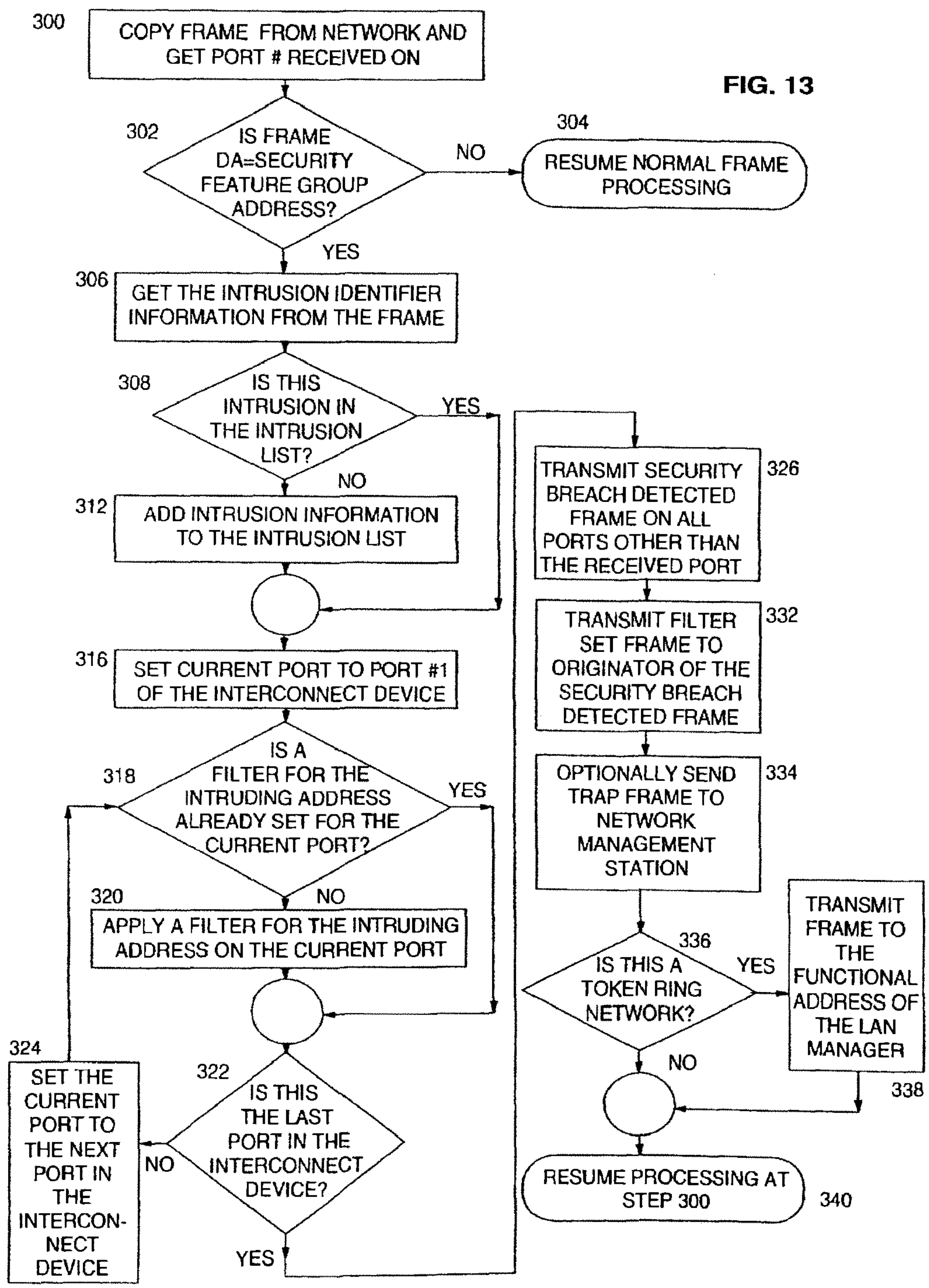

300
COPY FRAME FROM NETWORK AND GET PORT # RECEIVED ON
302
IS FRAME DA=SECURITY FEATURE GROUP ADDRESS?
NO
304
RESUME NORMAL FRAME PROCESSING
YES
306
GET THE INTRUSION IDENTIFIER INFORMATION FROM THE FRAME
308
IS THIS INTRUSION IN THE INTRUSION LIST?
YES
NO
312
ADD INTRUSION INFORMATION TO THE INTRUSION LIST
316
SET CURRENT PORT TO PORT #1 OF THE INTERCONNECT DEVICE
318
IS A FILTER FOR THE INTRUDING ADDRESS ALREADY SET FOR THE CURRENT PORT?
YES
NO
320
APPLY A FILTER FOR THE INTRUDING ADDRESS ON THE CURRENT PORT
322
IS THIS THE LAST PORT IN THE INTERCONNECT DEVICE?
NO
YES
324
SET THE CURRENT PORT TO THE NEXT PORT IN THE INTERCON-NECT DEVICE
326
TRANSMIT SECURITY BREACH DETECTED FRAME ON ALL PORTS OTHER THAN THE RECEIVED PORT
332
TRANSMIT FILTER SET FRAME TO ORIGINATOR OF THE SECURITY BREACH DETECTED FRAME
334
OPTIONALLY SEND TRAP FRAME TO NETWORK MANAGEMENT STATION
336
IS THIS A TOKEN RING NETWORK?
YES
TRANSMIT FRAME TO THE FUNCTIONAL ADDRESS OF THE LAN MANAGER
338
NO
RESUME PROCESSING AT STEP 300
340

FIG. 13

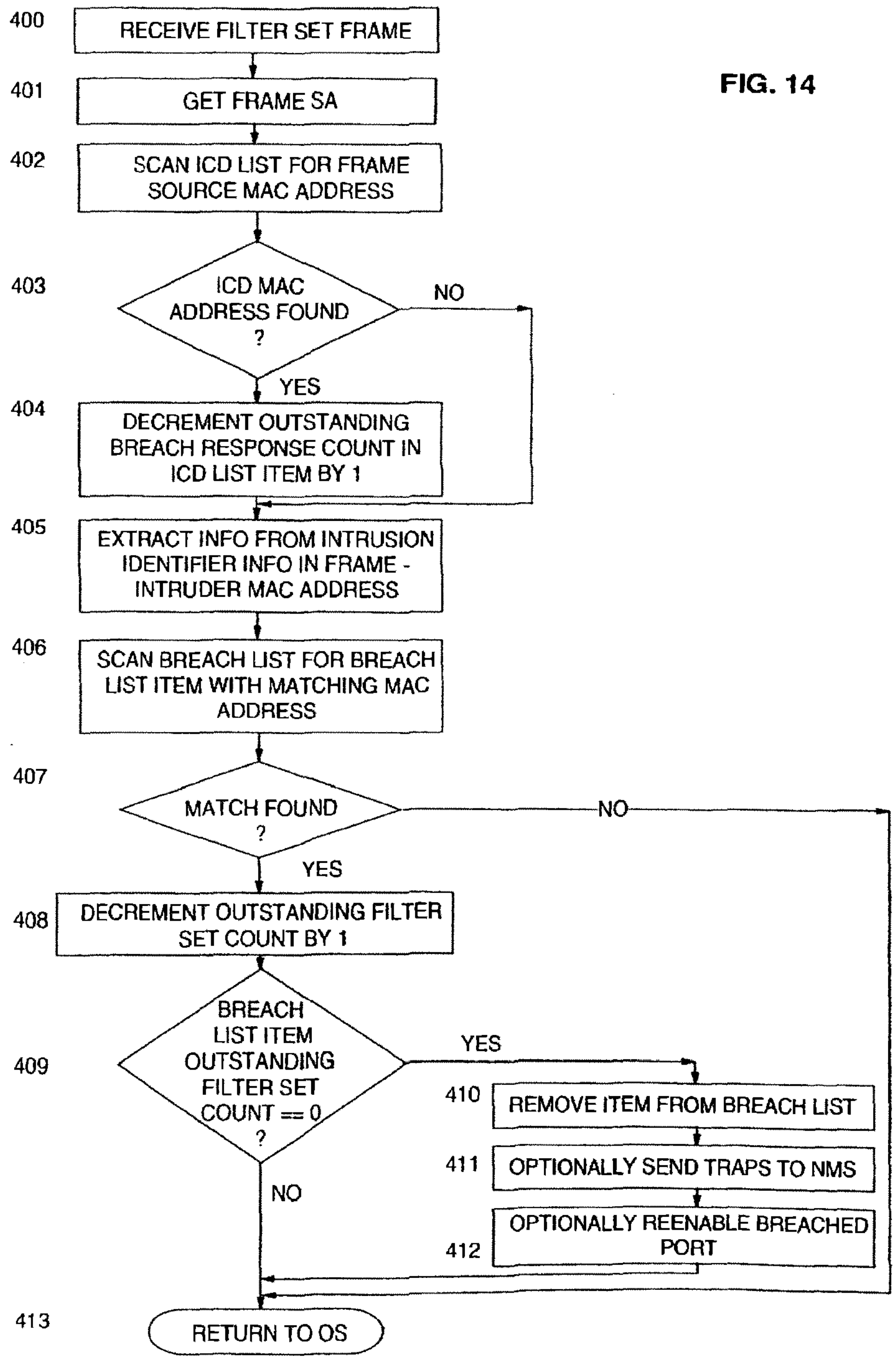

400
RECEIVE FILTER SET FRAME
401
GET FRAME SA
402
SCAN ICD LIST FOR FRAME SOURCE MAC ADDRESS
403
ICD MAC ADDRESS FOUND ?
NO
YES
404
DECREMENT OUTSTANDING BREACH RESPONSE COUNT IN ICD LIST ITEM BY 1
405
EXTRACT INFO FROM INTRUSION IDENTIFIER INFO IN FRAME - INTRUDER MAC ADDRESS
406
SCAN BREACH LIST FOR BREACH LIST ITEM WITH MATCHING MAC ADDRESS
407
MATCH FOUND ?
NO
YES
408
DECREMENT OUTSTANDING FILTER SET COUNT BY 1
409
BREACH LIST ITEM OUTSTANDING FILTER SET COUNT == 0 ?
YES
NO
410
REMOVE ITEM FROM BREACH LIST
411
OPTIONALLY SEND TRAPS TO NMS
412
OPTIONALLY REENABLE BREACHED PORT
413
RETURN TO OS

FIG. 14

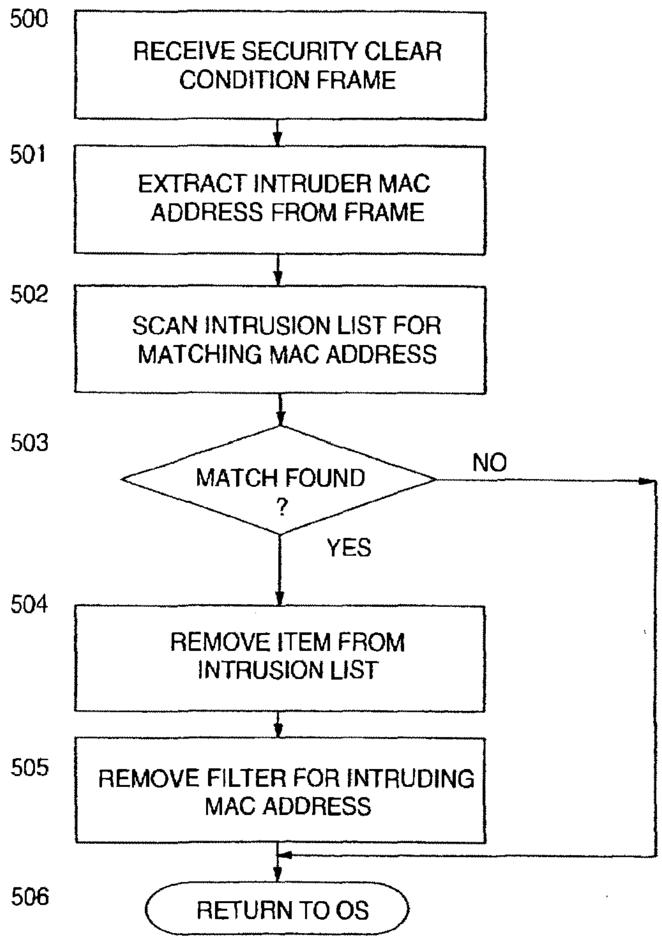

500
RECEIVE SECURITY CLEAR CONDITION FRAME
501
EXTRACT INTRUDER MAC ADDRESS FROM FRAME
502
SCAN INTRUSION LIST FOR MATCHING MAC ADDRESS
503
MATCH FOUND ?
NO
YES
504
REMOVE ITEM FROM INTRUSION LIST
505
REMOVE FILTER FOR INTRUDING MAC ADDRESS
506
RETURN TO OS

FIG. 15

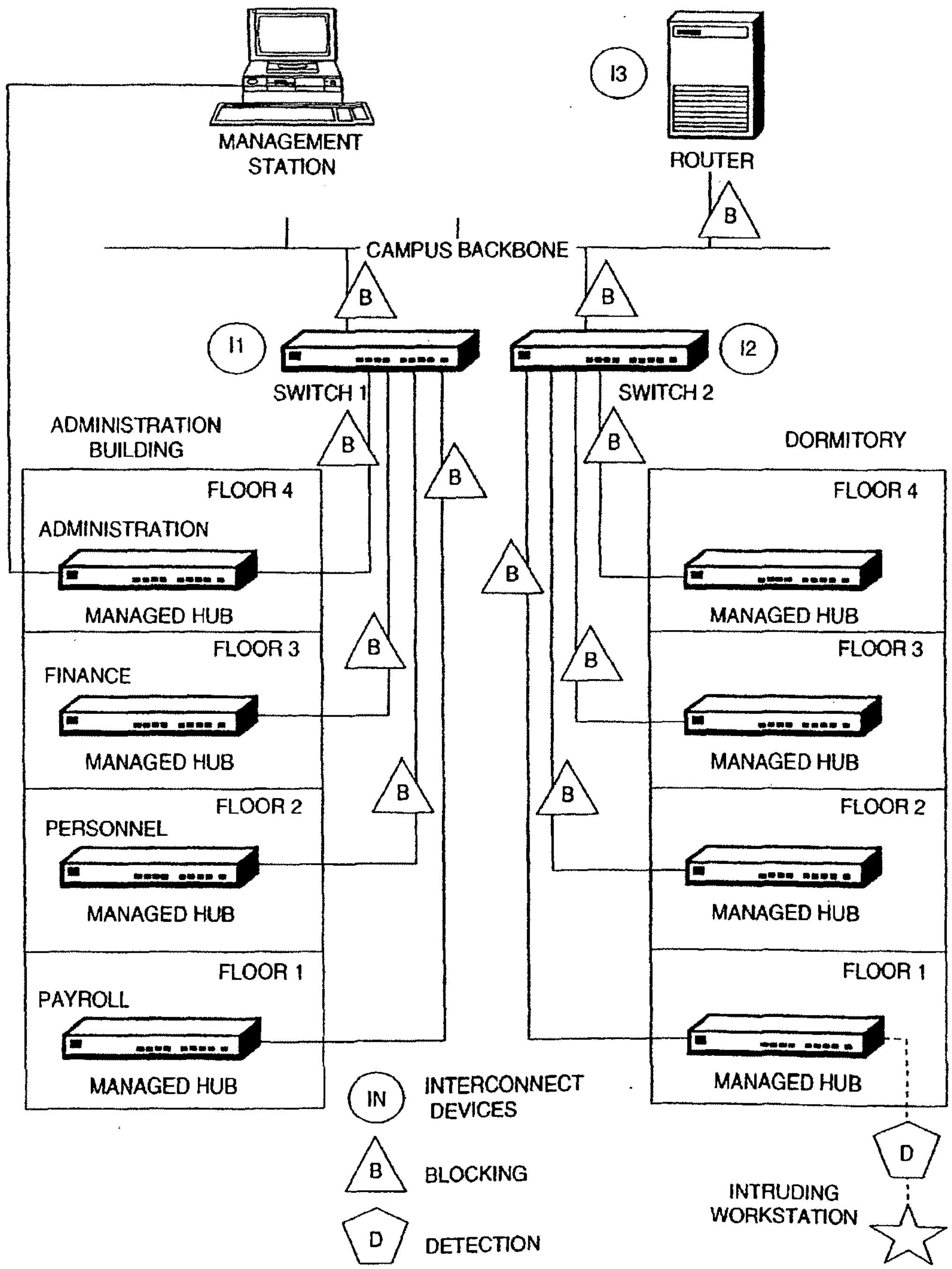

MANAGEMENT STATION
I3
ROUTER
B
CAMPUS BACKBONE
B
B
I1
SWITCH 1
SWITCH 2
I2
ADMINISTRATION BUILDING
B
B
DORMITORY
FLOOR 4
ADMINISTRATION
MANAGED HUB
FLOOR 3
FINANCE
MANAGED HUB
FLOOR 2
PERSONNEL
MANAGED HUB
FLOOR 1
PAYROLL
MANAGED HUB
B
B
B
B
B
B
FLOOR 4
MANAGED HUB
FLOOR 3
MANAGED HUB
FLOOR 2
MANAGED HUB
FLOOR 1
MANAGED HUB
IN
INTERCONNECT DEVICES
B
BLOCKING
D
DETECTION
D
INTRUDING WORKSTATION

FIG. 16

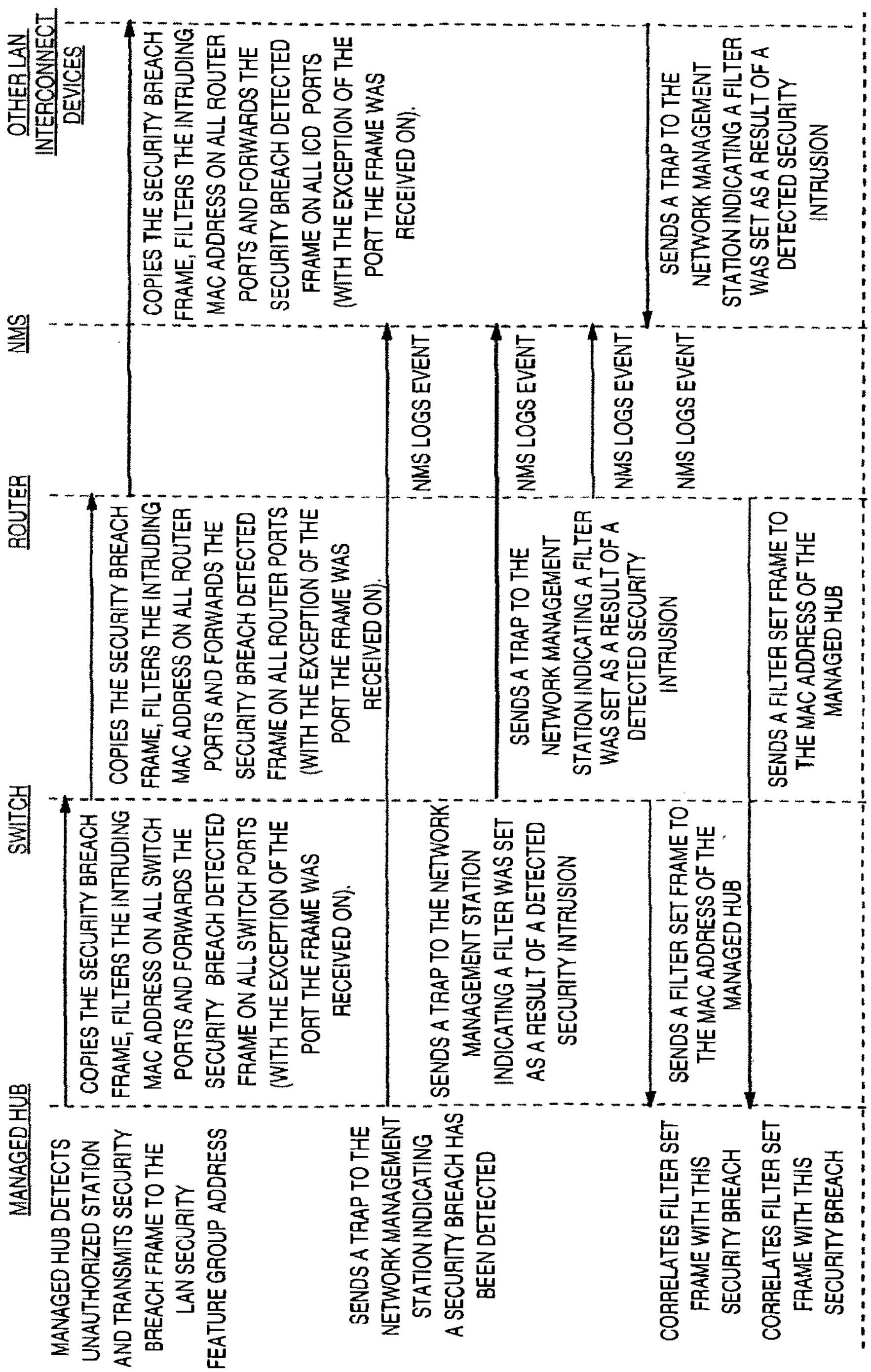

MANAGED HUB
SWITCH
ROUTER
NMS
OTHER LAN INTERCONNECT DEVICES
MANAGED HUB DETECTS UNAUTHORIZED STATION AND TRANSMITS SECURITY BREACH FRAME TO THE LAN SECURITY FEATURE GROUP ADDRESS
COPIES THE SECURITY BREACH FRAME, FILTERS THE INTRUDING MAC ADDRESS ON ALL SWITCH PORTS AND FORWARDS THE SECURITY BREACH DETECTED FRAME ON ALL SWITCH PORTS (WITH THE EXCEPTION OF THE PORT THE FRAME WAS RECEIVED ON).
COPIES THE SECURITY BREACH FRAME, FILTERS THE INTRUDING MAC ADDRESS ON ALL ROUTER PORTS AND FORWARDS THE SECURITY BREACH DETECTED FRAME ON ALL ROUTER PORTS (WITH THE EXCEPTION OF THE PORT THE FRAME WAS RECEIVED ON).
COPIES THE SECURITY BREACH FRAME, FILTERS THE INTRUDING MAC ADDRESS ON ALL ROUTER PORTS AND FORWARDS THE SECURITY BREACH DETECTED FRAME ON ALL ICD PORTS (WITH THE EXCEPTION OF THE PORT THE FRAME WAS RECEIVED ON).
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING A SECURITY BREACH HAS BEEN DETECTED
NMS LOGS EVENT
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING A FILTER WAS SET AS A RESULT OF A DETECTED SECURITY INTRUSION
NMS LOGS EVENT
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING A FILTER WAS SET AS A RESULT OF A DETECTED SECURITY INTRUSION
NMS LOGS EVENT
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING A FILTER WAS SET AS A RESULT OF A DETECTED SECURITY INTRUSION
NMS LOGS EVENT
CORRELATES FILTER SET FRAME WITH THIS SECURITY BREACH
SENDS A FILTER SET FRAME TO THE MAC ADDRESS OF THE MANAGED HUB
CORRELATES FILTER SET FRAME WITH THIS SECURITY BREACH
SENDS A FILTER SET FRAME TO THE MAC ADDRESS OF THE MANAGED HUB

FIG. 17A

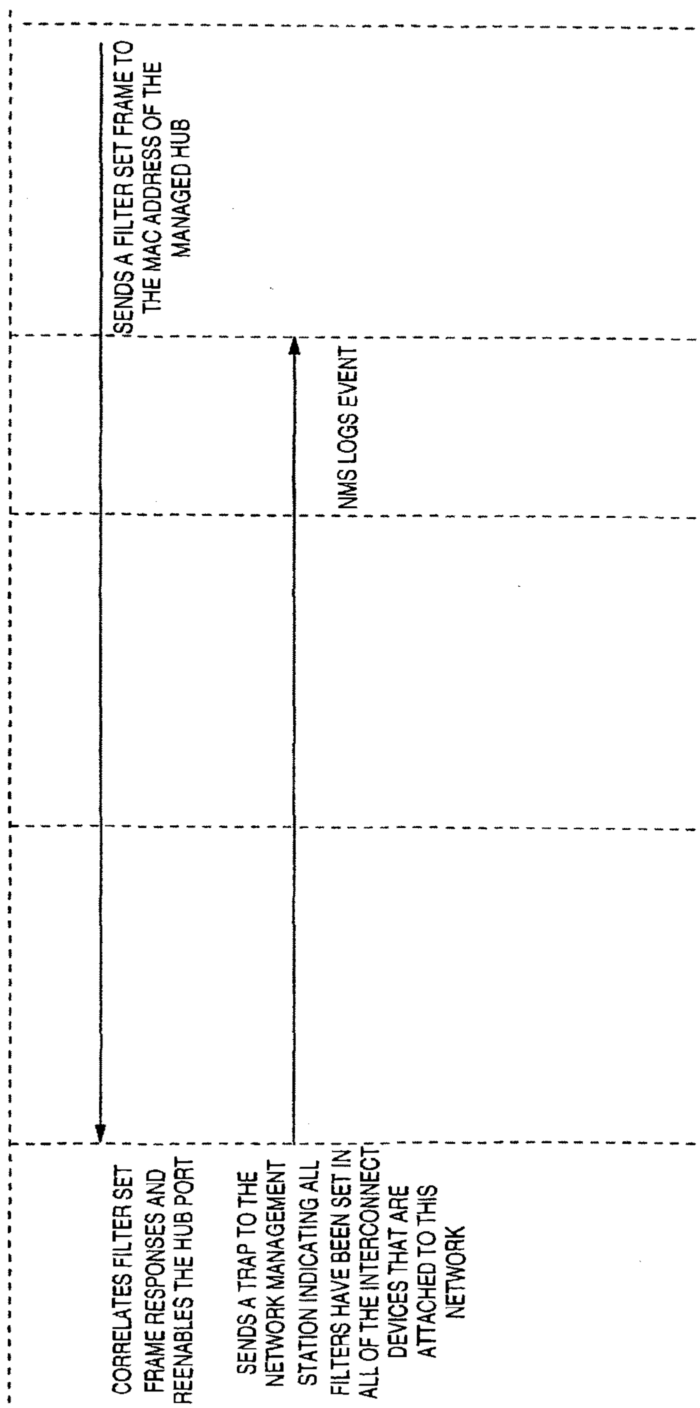

SENDS A FILTER SET FRAME TO THE MAC ADDRESS OF THE MANAGED HUB
NMS LOGS EVENT
CORRELATES FILTER SET FRAME RESPONSES AND REENABLES THE HUB PORT
SENDS A TRAP TO THE NETWORK MANAGEMENT STATION INDICATING ALL FILTERS HAVE BEEN SET IN ALL OF THE INTERCONNECT DEVICES THAT ARE ATTACHED TO THIS NETWORK

FIG. 17B

SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY

REFERENCE TO RELATED APPLICATION

This application is related to the following application having the same assignee and inventorship and containing common disclosure, and is believed to have an identical effective filing date: "Managed Network Device Security Method and Apparatus", U.S. application Ser. No. 08/775,536 filed Jan. 7, 1997.

BACKGROUND OF THE INVENTION

This invention relates in general to computer network security systems and in particular to systems and methods for detecting and preventing intrusion into a campus local area network by an unauthorized user.

As local area networks (LANs) continue to proliferate, and the number of personal computers (PCs) connected to LANs continue to grow at a rapid pace, network security becomes an ever increasing problem for network administrators. As the trend of deploying distributed LANs continues, this provides multiple access points to an enterprise's network. Each of these distributed access points, if not controlled, is a potential security risk to the network.

To further illustrate the demand for improved network security, an IDC report on network management, "LAN Management: The Pivotal Role of Intelligent Hubs", published in 1993, highlighted the importance of network security to LAN administrators. When asked the importance of improving management of specific LAN devices, 75% of the respondents stated network security is very important. When further asked about the growing importance of network security over the next three years, many respondents indicated that it would increase in importance.

More recently, a request for proposal from the U. S. Federal Reserve specified a requirement that a LAN hub must detect an unauthorized station at the port level and disable the port within a 10-second period. Although this requirement will stop an intruder, there is an inherent weakness in this solution in that it only isolates the security intrusion to the port of entry. The rest of the campus network is unaware of an attempted break-in. The detection of the unauthorized station and the disabling of the port is the first reaction to a security intrusion, but many significant enhancements can be made to provide a network-wide security mechanism. Where the above solution stops at the hub/port level, this invention provides significant enhancements to solving the problem of network security by presenting a system wide solution to detecting and preventing security intrusions in a campus LAN environment.

In today's environment, network administrators focus their attention on router management, hub management, server management, and switch management, with the goals of ensuring network up time and managing growth (capacity planning). Security is often an afterthought and at best administrators get security as a by-product of employing other device functions. For example, network administrators may set filters at router, switch, or bridge ports for performance improvements and implicitly realize some level of security as a side effect since the filters control the flow of frames to LAN segments.

The problem with using filters is that their primary focus is on performance improvements, by restricting the flow of certain types of network traffic to specified LAN segments. The filters do not indicate how many times the filter has actually been used and do not indicate a list of the media access control (MAC) addresses that have been filtered. Therefore, filters do not provide an adequate detection mechanism against break-in attempts.

Another security technique that is commonly employed in hubs is intrusion control. There are token ring and Ethernet managed hubs that allow a network administrator to define, by MAC address, one or more authorized users per hub port. If an unauthorized MAC address is detected at the hub port, then the port is automatically disabled. The problem with this solution is that prevention stops at the hub and no further action is taken once the security intrusion has been detected. This solution does not provide a network-centric, system-wide solution. It only provides a piecemeal solution for a particular type of network hardware namely, the token ring and Ethernet managed hubs. The result is a fragmented solution, where security may exist for some work groups that have managed hubs installed, but not for the entire campus network. At best, the security detection/prevention is localized to the hub level and no solution exists for a network-wide solution.

Other attempts to control LAN access have been done with software program products. For example, IBM Corporation's Lan Network Management (LNM) products LNM for OS2 and LNM for AIX both provide functions called access control to token ring LANs. There are several problems with these solutions. One problem with both of these solutions is that it takes a long time to detect that an unauthorized station has inserted into the ring. An intruder could have ample time to compromise the integrity of a LAN segment before LNM could take an appropriate action. Another problem with the LNM products is that once an unauthorized MAC address has been detected, LNM issues a remove ring station MAC frame. Although this MAC frame removes the station from the ring, it does not prevent the station from reinserting into the ring and potentially causing more damage. Because these products do not provide foolproof solutions, and significant security exposure still exists, they do not provide a viable solution to the problem of network security for campus LAN environments.

Thus, there is a need for a mechanism that ties together all of the piecemeal solutions into a comprehensive system solution that not only provides for detection of security intrusions, but also provides the proactive actions needed to stop the proliferation of security intrusions over the domain of an entire campus network.

SUMMARY OF THE INVENTION

It is, therefore, an object of the invention to provide a system and method for detecting and preventing security intrusions in a computer network.

It is another object of this invention to provide a system and method for detecting and preventing security intrusions in a local area network containing multiple managed devices.

It is a further object of this invention to provide a system and method for detecting and preventing security intrusions in a computer network having a managed hub and at least one interconnect device, such as a router, switch or bridge.

Overall, this invention can be described in terms of the following procedures or phases: discovery, detection, prevention, hub enable, and security clear. During each of these phases, a series of frames are transmitted between the interconnect devices on a campus network. These frames are addressed to a group address (multicast address). This well known group address needs to be defined and reserved for the LAN security functions that are described herein. This group address will be referred to as LAN security feature group address throughout the rest of this description.

The campus LAN security feature relies on managed hubs discovering the interconnect devices in the campus LAN segment that support this LAN security feature. The term "LAN interconnect device" is used throughout this description to refer to LAN switches (token ring and Ethernet 10/100 Mbps), LAN bridges and routers. The managed hub maintains a list of authorized MAC addresses for each port in the managed hub. If the managed hub detects an unauthorized station connecting to the LAN, the hub disables the port and then transmits a security breach detected frame to the LAN security feature group address. Each of the LAN interconnect devices on the campus LAN segment copies the LAN security feature group address and performs the following steps: 1) set up filters to filter the intruding MAC address; 2) forward the LAN security feature group address to other segments attached to the LAN interconnect device; and 3) send an acknowledgement back to the managed hub indicating that the intruding address has been filtered at the LAN interconnect device. Once the managed hub receives acknowledgements from all of the interconnect devices in the campus LAN, the port where the security intrusion was detected is re-enabled for use. Another part of the invention provides a network management station with the capability to override any security filter that was set in the above process.

The following is a brief description of each phase in the preferred embodiment of the invention:

1. Discovery

In this phase, the managed hub determines the interconnect devices in the campus network that are capable of supporting the LAN security feature. The managed hub periodically sends a discovery frame to the LAN security feature group address. The managed hub then uses the responses to build and maintain a table of interconnect devices in the network that support the security feature.

2. Detection

In the detection phase, the managed hub compares the MAC addresses on each port against a list of authorized MAC addresses. If an unauthorized MAC address is detected, then the managed hub disables the port and notifies the other interconnect devices in the campus network by transmitting a security breach detected frame to the LAN security feature group address.

3. Prevention

The prevention phase is initiated when a LAN interconnect device receives the security breach detected frame. Once this frame is received, the LAN interconnect device sets up a filter to prevent frames with the intruding MAC address from flowing through this network device. The LAN interconnect device then forwards the security breach detected frame to the other LAN segments attached to the interconnect device. The LAN interconnect device also transmits a filter set frame back to the managed hub.

4. Hub Enable

The hub enable phase takes place when the managed hub has received all acknowledgements from the LAN interconnect devices in the campus network. When the acknowledgements have been received, the managed hub re-enables the port where the security intrusion occurred.

5. Security Clear Condition

In this phase, a network management station can remove a filter from a LAN interconnect device that was previously set in the prevention step.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described with respect to a preferred embodiment thereof which is further illustrated and described in the drawings.

FIG. 1 is a block diagram of a campus network in which the present invention can be implemented.

FIG. 2 is a component block diagram for an SNMP managed device.

FIG. 3 is a component block diagram for a network management station.

FIGS. 4A–4C show general frame formats for Ethernet and token ring frames.

FIGS. 5A–5E show the information contained in the Ethernet and token ring frame data fields to represent the different frame types that are implemented in the preferred embodiment.

FIG. 6 illustrates the structure of the Interconnect Device List (ICD).

FIG. 7 illustrates the structure of the Breach List.

FIG. 8 illustrates the structure of the Intrusion List.

FIG. 9 is a flow chart of the processing that occurs in the managed hub to initiate the discovery phase of the invention.

FIG. 10 is a flow chart of the processing that occurs in the interconnect device during the discovery phase of the invention.

FIG. 11 is a flow chart of the processing that occurs in the managed hub during the discovery phase of the invention in response to the receipt of a discovery response frame.

FIG. 12 is a flow chart of the processing that occurs in the managed hub during the detection phase of the invention.

FIG. 13 is a flow chart of the processing that occurs in an interconnect device during the prevention phase of this invention.

FIG. 14 is a flow chart of the processing that occurs in the managed hub during the hub enable phase of the invention.

FIG. 15 is a flow chart of the processing that occurs in the interconnect devices in response to the receipt of a security clear condition frame.

FIG. 16 is an example of the implementation of the invention in a campus LAN environment.

FIG. 17 is an example of the data flows corresponding to the example implementation in a campus LAN environment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The preferred embodiment of this invention uses the SNMP network management protocol, since SNMP is the most prevalent network management protocol in the industry and is the most widely deployed in campus networks. It should be noted that the concepts in this invention related to network management could also be applied to other network management protocols such as CMIP or SNA.

FIG. 1 illustrates a typical campus network environment in which the present invention can be implemented. As shown in the figure, the campus network 10 contains interconnect devices, such as router 12, router 14, token ring switch 16, bridge 18, managed hubs 20, 22, 24, network management station 26, workstation 28 and file server 30.

The managed hubs and interconnect devices depicted in FIG. 1 are considered SNMP managed devices. The typical component block diagram for an SNMP managed device is illustrated in FIG. 2. A typical managed device is an embedded system that includes a system bus 50, random access memory (RAM) 52, NVRAM 54 to store configuration information, FLASH EPROM 56 to store the operational and boot-up code, a processor or CPU 58 to execute the code instructions, and a media access control (MAC) chip 66 that connects the device to the network **10**. FIG. 2 also shows operational code **60**, TCP/IP protocol stack **62** and SNMP agent code **64**. In most instances, the operational code and the frame processing code execute in FLASH memory **56** or in RAM **52**. The code that implements several phases in this invention is included as a part of the operational code (microcode or firmware) of the managed device. The MAC chip **66** copies the frames corresponding to the different phases into RAM **52** and notifies the processor **58**, usually via an interrupt, that a frame is ready for processing. The operational code **60** handles the interrupt and processes the frame.

FIG. **3** illustrates the typical component block diagram for a network management station such as that indicated by reference numeral **26** in FIG. **1**. The network management station includes a processor **70**, with a system bus **90** to which RAM **72**, direct access storage device (DASD) **74**, other peripherals **76**, display monitor **78**, keyboard **80**, mouse **82** and network interface card **84** are connected.

FIGS. 4A–4C show the general frame formats for Ethernet and token ring frames. The LAN security feature group address is placed in the destination address (DA) field of the discovery request, security breach detected and security clear condition (optionally) frames as discussed more fully below. The data field portion of each frame is used to pass the additional information related to this security feature.

The following describes the information that is included in the data fields of the Ethernet and token ring frame types to represent the different frames that are specific to the preferred embodiment of the invention.

The discovery request frame shown in FIG. 5A is sent to the LAN security feature group address and the data field includes a one byte field which indicates that the frame type (frame type identifierx'01') is a discovery request frame. The time stamp field is the system time value when the discovery request frame is transmitted. It is used to correlate the discovery response frame with the discovery request frame.

The discovery response frame shown in FIG. 5B is sent to the individual MAC address of the managed hub that initiated the request. The data field in this frame includes a one byte field which indicates that the frame type is a discovery response frame (frame type identifierx'02'), and also contains the MAC address of the LAN interconnect device sending the frame, a description of the LAN interconnect device (e.g., IBM 8272 Model 108 Token Ring Switch), and a time stamp that is used to correlate the discovery response frame with the discovery request frame.

The security breach detected frame shown in FIG. 5C is sent to the LAN security feature group address and the data field includes a one byte field which indicates that the frame type is a security breach detected frame (frame type identifierx'03') and contains the MAC address that was detected as the security intruder. Other fields of this frame contain the module number and port number where the security breach was detected and the system time when the security breach was detected. When the time stamp value is used in combination with the intruding MAC address and module and port numbers, it forms an intrusion identifier as will be referred to subsequently. Following the time stamp are device field length indicating the length of the field that follows and address fields. The address field contains the list of addresses that have processed and forwarded the security breach detected frame. It starts with the originating MAC address of the managed hub. Each successive interconnect device that receives the frame, appends its MAC address to the end of this field and updates the device field length before it forwards the frame. It provides an audit trail or path that the security breach detected frame followed throughout the network. A network management station can monitor the progress of the security breach detected frame through information in the trap frames that it receives.

The filter set frame shown in FIG. 5D is sent to the individual MAC address of the managed hub that initiated the security intrusion condition. The data field includes a one byte field which indicates that the frame type is a filter set frame (frame type identifierx'04') and contains the MAC address of the LAN interconnect device sending the frame. Other fields in this frame are the MAC address of the detected intrusion, the module and port number of the managed hub where the security intrusion was detected, and the time stamp representing the system time when the security breach was detected.

The security clear condition frame shown in FIG. 5E can be sent to the LAN security feature group address or to the individual MAC address of a LAN interconnect device. The data field includes a one byte field which indicates that the frame type is a security clear condition frame (frame type identifierx'05') and contains the intruding MAC address to remove as a filter.

Trap frames are sent to the network management station at various times depending upon the phase of the invention that is being performed. All trap frames have the same basic format with the information in each trap frame varying according to the phase.

In the discovery phase, traps are sent as a result of the managed hub deleting an interconnect device from the list of devices that are in the security domain of interconnect devices. The discovery trap frame contains the trap identifier (x'01'), the MAC address of the interconnect device and device description. This trap indicates that an interconnect device was removed from a managed hub interconnect device list because it did not respond to the managed hub with a discovery response frame within the allotted time period of the discovery window.

Traps sent in the detection phase indicate that the managed hub detected an intrusion on one of the hub ports. Information in this trap frame includes trap identifier (x'02'), the MAC address of the intruding device, the module and port number of the detected intrusion, and the time when the security intrusion was detected.

Traps sent in the prevention phase indicate that the interconnect device has completed the processing of a received security breach detected frame. This trap frame contains the trap identifier (x'03'), the MAC address of the intruding device, the module and port number of the detected intrusion, the time when the security breach was detected and a variable length address field. This last field contains a list of MAC addresses for all the devices that have processed the security breach detected frame. This information provides to the network management station the path that the security breach detected frame followed through the network.

Traps sent in the hub enable phase indicate that the managed hub has reenabled a hub port as a result of receiving filter set frames from all of the interconnect devices in the discovered security domain, i.e., all the discovered interconnect devices. This trap frame contains the trap identifier (x'04'), the MAC address of the intruding device, the module and port number of the detected intrusion, and the time when the security breach was detected.

For token ring networks, the information in the trap frames can be included in frames addressed to the functional address of the LAN manager. The LAN management frame format and defined functional address are specified in the IBM Token Ring Network Architecture (SC30-3374-02) publication.

For managed hubs, the authorized address list (AAL) controls which MAC addresses are allowed to connect to specified ports. Each entry in the AAL consists of two fields: port number and authorized address. The port number identifies a specific port on the hub; the authorized address field specifies the address or addresses that are allowed to connect to the port.

The AAL can be built by the network administrator as part of the configuration of the managed hub. The network administrator identifies the addresses that are allowed to connect to specific ports on the hub. After the initial configuration, the AAL can be updated in several ways. The network management station can add or delete entries in the AAL by sending SNMP management frames. Since most managed hubs provide a Telnet interface into the device to change configuration parameters, a Telnet session could be used to add or delete entries in the AAL. Also, since most managed hubs provide for the attachment of a local console over an RS232 serial port connection which can be used to change configuration parameters, a local console session can be used to add or delete entries in the AAL.

Alternatively, the AAL can be built dynamically through a learning process. Most managed hubs provide a mechanism in the hardware to capture the addresses of the stations that are attached to the ports of a hub. These learned addresses can be provided to the network management station as those stations authorized to access the hub. These learned addresses are then used as the AAL for the managed hub.

The discovery phase is initiated by each managed hub in the campus network. Its purpose is to determine the LAN interconnect devices in the campus LAN that support the LAN security feature. Each managed hub periodically transmits a discovery frame (FIG. 5A) to the LAN security feature group address. The managed hub then uses the information in the response frame (FIG. 5B) to build and maintain a list of all of the devices that support the LAN security feature. This list is referred to as the Interconnect Device List (ICD). The addresses in this list are used in the hub enable phase to correlate the reception of the filter set frame (FIG. 5D) with entries in the list. The managed hubs typically store these ICD lists in management information base (MIB) tables where they can be retrieved, upon request, from a network management station.

The discovery phase can also be used to provide an integrity check on the ICD list of devices supporting the LAN security feature. By periodically transmitting the discovery frame (FIG. 5A) to the LAN security feature group address, checks can then be made to ensure that all of the devices are still in the ICD security list. If any discrepancies are detected, e.g., if a station is removed from the list or added to the list, then an SNMP trap is sent to the network management station. This notification alerts the network administrator that a potential security exposure exists in the campus network. FIG. 6 illustrates the structure of the ICD list along with the information stored in the list for each discovered interconnect device. Other lists that are built and maintained in the detection and prevention phases are the Breach List shown in FIG. 7 and the Intrusion List shown in FIG. 8. Their use will be explained below in the description of the detection and prevention phases.

The detection phase operates at the managed hub level. Each port on the managed hub can be configured to hold one or more MAC addresses of users that are authorized to access the network. The managed hubs can be 10 or 100 Mbps Ethernet or token ring hubs. Current hub chipsets provide the capability to determine the last source MAC address that is seen on a port. When a station attempts to connect to a network, either by inserting into the token ring or by establishing a link state with an Ethernet hub, the last source address seen on the port is compared to the authorized list of MAC addresses that has been defined for this port. If the address is authorized then normal network operations occur. If the address is not authorized, then the managed hub performs the following actions:

1. disables the port;
2. sends an SNMP trap frame to the network management station;
3. sends an alert frame to the functional address of the LAN Manager (token ring); and
4. transmits a security breach detected frame (FIG. 5C) to the LAN security feature group address.

Additional variables in the SNMP trap provide information about the point of intrusion: e.g. the module id (in the case of stackable hubs), the port number, the network number (in cases where hubs have multiple backplanes), and a time stamp (sysUpTime) of when the intrusion was detected. SysUpTime is an SNMP MIB variable that represents the time (units of 0.01s) since the network management portion of the system was last reinitialized.

Some managed hubs support multiple backplanes or networks. In this case, the security breach detected frame is transmitted on all of the active backplanes/networks within the hub.

The well known group address needs to be defined and reserved for LAN security functions. The security breach detected frame (FIG. 5C) containing the MAC address of the station that intruded into the network is sent to the LAN security feature group address.

The prevention phase spans the network. Each interconnect device in the campus network is configured to copy frames addressed to the LAN security feature group address. Upon a security intrusion, the network interconnect devices copy the security breach detected frame (FIG. 5C) and perform the following functions:

1. set filters based on the intruder's MAC address.
2. transmit a security breach detected frame (FIG. 5C) to the LAN security feature group address.
3. send an SNMP trap frame to the network management station.
4. send an alert frame to the functional address of the LAN manager (token ring).
5. transmit filter set frame (FIG. 5D) to the MAC address of the hub that initiated the security breach process.

Setting filters by the network interconnect device prevents intrusion attempts with this MAC address originating elsewhere in the campus network from flowing through this interconnect device. This protects an enterprise's data on this segment of the network from any attacks via the intruder's MAC address.

The interconnect device extracts the intrusion identifier information from the security breach detected frame. If this is the first time the interconnect device has received a security breach detected frame with this intrusion identifier, the interconnect device adds this information to the Intrusion List, then checks to ensure the filter has been set for the intruding MAC address and resets, if required. The interconnect device then transmits the security breach detected frame on all ports except the port on which the security breach detected frame was received.

Sending the trap frame indicates that the filter has been set as a result of receiving the security breach detected frame. Likewise, sending the alert frame indicates that the filter has been set as a result of receiving the security breach detected frame.

The hub enable phase operates at the network level. The hub that initiates the security breach process receives the filter set frames from the interconnect devices in the campus network. The hub then waits to receive responses back from all of the interconnect devices that were determined in the discovery phase to be in the campus network. When all the interconnect devices in the network have responded to the hub with the filter set frame, the hub then re-enables the port for use and then sends a TRAP frame back to the network management station indicating that all filters have been set for the intruding MAC address. The network management station can optionally forward this information to a network management application such as IBM Corporation's NetView/390 product via an alert.

The security clear condition phase of this invention provides the capability for a network administrator to manually override, if necessary, one of the filters that has been set in the prevention phase. The network management station could globally clear, i.e., remove a filter from all LAN interconnect devices by transmitting the security clear condition frame (FIG. 5E) to the LAN security feature group address. The network management station could selectively clear, i.e., remove a filter from a LAN interconnect device by transmitting the security clear condition frame to the MAC address of the specific LAN interconnect device.

FIGS. 9–15 are flow charts that illustrate the processing that occurs in the managed hub and in the interconnect devices during each phase of the invention. The code to implement the discovery phase of this invention runs within the managed hub and interconnect device as event driven threads within the realtime OS embedded system. The flows in FIG. 9 depict the processing that occurs in the managed hub to initiate each discovery phase. This task manages the initialization and update of the Interconnect Device List and timing of the next iteration of the discovery phase. The following briefly describes each logic block in the figure.

Step **100**: Entry to this task can be caused by a power on and/or reset. This would be one of many tasks that would run in response to this event.

Step **101**: There are two lists, a period, a window, and two flags that are used by the managed hub in this invention. The ICD (Interconnect Device) List contains information on the devices found during the discovery phase. The Breach List contains information on intrusions recognized by the hub and in the process of being secured. The period is the time between discovery phases. The window is the time between when a discovery phase is initiated and when an Interconnect Device must respond before being assumed inaccessible due to network or device outage. One flag is an indication that initialization has completed. The other flag is an indication that the security feature is enabled. The lists, the period, the window and the enabled flag may be cleared or loaded from persistent memory. The initialized flag is set to True.

Step **102**: Test for whether the security feature is enabled.

Step **103**: Each managed hub maintains a MIB variable that is called SysUpTime. This is used as a time stamp for security feature frames.

Step **104**: The discovery frame is built with the data field containing the type of the frame—Request.

Step **105**: The frame is sent to the LAN security feature group address.

Step **106**: The discovery phase is initiated periodically as an integrity check on the security feature coverage within the network. The period is adjustable to reflect variable path lengths or round-trip-times between a managed hub and interconnect devices. The period can be set via SNMP. The longer the period, the less the integrity of the network coverage. The shorter the period, the higher the traffic rate required for the security feature.

Step **107**: Set a pointer to the head of the list of ICD (Interconnect Device) List items. The pointer may point to an item or nothing if there are not items in the list. (The ICD List is a list of the interconnect devices that responded in a previous discovery phase). This part of the task is to update the Interconnect Device List by updating items as appropriate or deleting them as necessary.

Step **108**: Does the pointer point to an item in the list or does it point beyond the end of the list?

Step **109**: Each ICD List item has a time stamp from the last discovery response frame received from the device.

Step **110**: Is the time for the item in the ICD List later than current time?

Step **111**: If yes, the managed hub has reset or rolled over its SysUpTime since the last response from the ICD. Set the time in the ICD List item to current time.

Step **112**: Is the difference between the current time and the last response time from the item greater than the discovery window?

Step **113**: Assume the device is inaccessible due to network or device outage and purge the item from the ICD List. Also, decrement the outstanding filter set count on all the Breach List items.

Step **114**: If there is a network management station (NMS) that is receiving traps from the managed hub and the traps are enabled, send a trap indicating that the interconnect device is no longer accessible. If there is an LNM for OS/2 station available and traps are enabled, send a trap to the LNM for OS/2 station.

Step **115**: Move the ICD List pointer to the next item or to the end of the list if no more entries exist. This is for stepping through the entire list of ICD items.

Step **116**: End the task and return to the embedded system OS.

Step **117**: Enter this task due to a timer driven interrupt (set in step **106**).

The flows in FIG. **10** depict the processing that occurs in the interconnect devices during each iteration of the discovery phase. This task responds to the receipt of a discovery request frame by sending a discovery response frame. The following briefly describes each logic block in the figure.

Step **143**: The task is initiated by the receipt of a discovery request frame.

Step **144**: A check is made for whether the security feature is enabled. This determines if any additional processing is required.

Step **145**: The source MAC address and time stamp are extracted for building the response.

Step **146**: The discovery response frame is built using the information from the discovery request frame that was just received.

Step 147: The frame is sent to the originating managed hub.

Step 148: The task ends, returning control to the embedded OS.

The flows in FIG. 11 depict the processing that occurs in the managed hub in response to the receipt of a discovery response frame. This task maintains the state of this iteration of the discovery phase. The following briefly describes each logic block in the figure.

Step 130: The task is initiated in the managed hub by the receipt of a discovery response frame.

Step 131: The interconnect device information is extracted from the frame.

Step 132: The Interconnect Device List is searched for an item with a MAC address matching the source address of the discovery response frame.

Step 133: Has a match been found?

Step 134: If a match is found, update the last response time in the ICD List item with the time stamp that was extracted from the discovery response frame.

Step 135: If there is no match, assume that the device is not in the list because of either network/device outages or the device has just started utilizing the security feature. It is necessary to determine if the discovery window is still large enough. The round-trip-time is calculated, and multiplied by 2 to derive a potential discovery window. If this is larger than the current discovery window, the discovery window needs to be changed.

Step 136: Change the discovery window.

Step 137: Create a new Interconnect Device List item using the source address from the discovery response frame, the device description from the frame, and the time stamp from the frame. Add it to the list.

Step 138: Optionally send a trap to the network management station(s) and if this is a token ring, to the LAN manager functional address.

Step 139: The task ends, returning control to the embedded OS.

The code to implement the detection phase of this invention runs as a separate task independent from the other tasks in the managed hub. The flows in FIG. 12 depict the processing that occurs during the dispatch of the detection phase task. This task simply checks all the ports in the hub to ensure that the station attached to the port has been authorized to establish a connection on this port. The AAL (Authorized Address List) defines which MAC addresses are allowed to connect to specific ports on the hub. The following briefly describes each logic block in the figure.

Step 200: This is the entry point for the detection phase task. Processing starts at port number 1 in the hub and continues until all of the ports in the hub have been processed.

Step 210: This step checks if a station is attached to the port in the hub. If a station is attached, then an address exists for the port. If an address is detected for the port (i.e., a station is attached to the port), then processing continues with step 220. If there is no address detected for this port (i.e., no station is attached), then processing continues with step 230.

Step 220: A check is made here to ensure that the address that has been detected on this port is in the list of authorized addresses. If the address detected on the port is authorized, then continue processing at step 230. If the address detected on the port is not in the authorized list, then processing continues at step 250.

Step 230: A check is made here to see if all of the ports in the hub have been processed. If all of the ports have been processed, then processing resumes at step 200 with the processing of port number 1. If this was not the last port and there are more ports to process, then processing continues at step 240.

Step 240: In this step, the next port in the hub is set up to be processed. Processing then continues at step 210.

Step 250: In this step a check is made to see if the port is already disabled. If the port is already disabled, then the port/network is already secure from intruders on this port. If the port is already disabled, then processing continues at step 230. If the port is enabled, processing then continues at step 260.

Step 260: In this step, the port is disabled. Processing then continues at step 265.

Step 265: In this step, an entry is added to the Breach List containing the following: MAC address that was detected as the intruder, the module and port number where the intrusion was detected, the time (sysUpTime) when the security breach was detected, and the outstanding filter set count which is set to the number of entries in the ICD list. Processing then continues at step 270.

Step 270: In this step, the security breach detected frame is transmitted on all network segments of the hub. The info field of the security breach detected frame includes the following: MAC Address of the intruder, module number, port number, time stamp (sysUpTime), the device field length initialized to 6 (bytes), the 6 byte MAC address of the managed hub. Processing then continues at step 280.

Step 280: In this step, a trap frame is optionally sent to the network management station. The trap frame includes the following information:

(a) trap identifierx'02';

This indicates that the managed hub detected in intrusion on one of the hub ports.

(b) MAC address of the intruding device;

(c) module number of the detected intrusion;

(d) port number of the detected intrusion;

(e) time when the security breach was detected;

Processing then continues at step 290.

Step 290: In this step, a check is made to see if this invention has been implemented in a token ring network. The token ring architecture defines a special functional address that is used by LAN management stations. Functional addresses are only used in token ring environments. If the invention is implemented in a token ring network, processing then continues at step 295. If the invention is implemented in a non-token ring network, processing then continues at step 230.

Step 295: In this step, a frame is sent to the functional address of the LAN manager with the information from step 280. Processing then continues at step 230.

FIG. 13 depicts the flows for the prevention phase of the invention. The prevention phase is implemented in the interconnect devices of the network. The following briefly describe each logic block in the figure.

Step 300: The processing is initiated when the interconnect device receives a frame from the network. The interconnect device copies the frame and saves the port number that the frame was received on. Processing then continues at step 302.

Step 302: In this step, the frame that was copied in step 300 is interrogated and a check is made to determine if the destination address of the frame is equal to the LAN security feature group address. If the received frame is addressed to the LAN security feature group address, then processing continues at step 306. Otherwise, the frame is of some other type and the processing continues with step 304.

Step 304: This step is encountered for all frame types other than the LAN security feature. The normal frame processing code of the interconnect device runs here.

Step 306: In this step, the intrusion identifier information is copied from the frame. The intrusion identifier consists of the following information:

(a) MAC address of the intruder;

(b) module number;

(c) port number;

(d) time stamp;

Processing then continues at step 308.

Step 308: In this step, a check is made to determine if the intrusion identifier is already in the Intrusion List of this interconnect device. If yes, processing then continues at step 316. If no, processing then continues at step 312.

Step 312: In this step, the intrusion identifier information is added to the Intrusion List. Processing then continues at step 316.

Step 316: In this step, the current port of the interconnect device is set to port number 1. Processing then continues at step 318.

Step 318: In this step, a check is made to determine if the intruding MAC address is already filtered on the current port. If yes, processing then continues at step 322. If no, processing then continues at step 320.

Step 320: In this step, a filter is set for the intruding MAC address on the current port. Processing then continues at step 322.

Step 322: In this step a check is made to determine if the filter processing has been applied to all of the ports in the interconnect device. If all of the ports have been processed, processing then continues at step 326. If there are more ports to process, processing then continues at step 324.

Step 324: In this step, the current port is set to the next port in the interconnect device. Processing then continues at step 318.

Step 326: In this step, the security breach detected frame is propagated throughout the network. The interconnect device transmits the security breach detected frame on all ports other than the port the original frame was received on. (Reference step 300 where it is determined which port the frame was received on). Before transmitting the security breach detected frame, the ICD appends its MAC address to the addresses field of the frame and increments the device field length field of the frame by 6. This provides the audit trail or the path information for the security breach detected frame. Processing then continues at step 332.

Step 332: In this step, the interconnect device transmits the filter set frame to the originator of the security breach detected frame. The originator is determined by extracting the source address from the frame that was copied in step 306. Processing then continues at step 334.

Step 334: In this step, a trap frame is sent to the network management station. The trap frame includes the following information:

(a) trap identifierx'03';

This indicates that the interconnect device has completed the processing of a received security breach detected frame.

(b) MAC address of the intruding device;

(c) module number of the detected intrusion;

(d) port number of the detected intrusion;

(e) time when the security breach was detected;

(f) addresses field;

This is a variable length field that contains a list of all of the devices that have processed the security breach detected frame. This information provides to the network management station the path that the security breach detected frame followed throughout the network.

Processing then continues at step 336.

Step 336: In this step, a check is made to see if this invention has been implemented in a token ring network. The token ring architecture defines a special functional address that is used for LAN management stations. Functional addresses are only used in token ring environments. If the invention is implemented in a token ring network, processing then continues at step 338. If the invention is implemented in a non-token ring network, processing then continues at step 340.

Step 338: In this step, a frame containing the same information in the trap frame in step 334 is sent to the functional address of the LAN manager. Processing then continues at step 340.

Step 340: In this step, processing resumes again at step 300.

The code to implement the hub enable phase of this invention runs within the managed hub as event driven threads within the realtime OS embedded system. The flows in FIG. 14 depict the processing that occurs in the managed hub in response to receipt of each filter set frame. The task maintains the necessary lists of interconnect devices and breaches to complete the hub enable phase for each breach. The following briefly describes each logic block in the figure.

Step 400: The task is initiated in the managed hub by the receipt of a filter set frame.

Step 401: Get the source address of the frame for finding the associated ICD List item.

Step 402: The Interconnect Device List is scanned for an item with the same MAC address as the source address of the frame.

Step 403: Was a match found? If not, assume that the interconnect device is no longer accessible.

Step 404: If a match is found, decrement the outstanding breach response count in ICD List item by 1. This provides an up-to-date count of outstanding responses for each ICD.

Step 405: Extract intrusion identifier information from the frame.

Step 406: Scan the Breach List for an item with a matching intrusion identifier.

Step 407: Match found?

Step 408: If a match is found, decrement the outstanding filter set count by 1 in the matching Breach List item.

Step 409: Have all interconnect devices responded? Are all filters set?

Step 410: Since the intruder is now being filtered and has been removed from the network, remove the Breach List item.

Step 411: If there is a listening network management station(s), send a trap. If this is a token ring, send an alert to the LAN manager functional address.

Step 412: Optionally reenable the port. This is a policy decision. It may also reflect the likelihood of the intruder still attempting to intrude via this same port.

Step 413: End the task and return control to the embedded OS.

The code to implement the security clear condition phase of this invention runs within the interconnect devices as event driven threads within the realtime OS embedded system. The flows in FIG. 15 define the processing that occurs in the interconnect devices in response to receipt of each security clear condition frame. The task updates the Intruder List of breaches and completes the security clear condition phase for each breach. The following briefly describes each logic block in the figure.

Step 500: The task is initiated in the interconnect device by the receipt of a security clear condition frame from a network management station.

Step 501: Extract the intruder MAC address from the security clear condition frame.

Step 502: Search the Intrusion List for a matching MAC address.

Step 503: Is there a match?

Step 504: If there is a match, remove the item from the Intrusion List.

Step 505: Remove filter for the intruding MAC address.

Step 506: End the task and return control to the embedded OS.

Two examples are given below to illustrate the actions that are performed by the managed hub and interconnect devices in an implementation of this invention in an operational campus environment. Referring again to FIG. 1, there is depicted a workstation 28, attached to an Ethernet hub 24, that is attempting to gain unauthorized access to a file server 30 that is located on a token ring segment. The security intrusion is detected by the managed Ethernet hub 24, since the MAC address of the workstation 28 is not authorized for this port in the hub. The managed hub 24 then disables the port and transmits the security breach detected frame to the LAN interconnect device 14 on this segment, which, in turn, forwards the security breach detected frame to LAN interconnect devices 12, 16 that are attached to subnet 3 and subnet 4, respectively. LAN interconnect device 12, in turn, forwards the security breach detected frame to LAN interconnect device 18. The LAN interconnect devices 12, 14, 16, 18 set filters on all ports in the device to prevent frames with the intruding MAC address from flowing through the interconnect device.

More specifically, the managed hub 24 disables the port and transmits the security breach detected frame to router 14. The managed hub 24 also sends a trap frame to the management station 26. Router 14 applies the intruder's MAC address as a filter on all of its ports and forwards the security breach detected frame on all of its ports, except the port the security breach detected frame was received on. Router 14 then sends a trap to the network management station 26 and sends a filter set frame back to the managed hub 24. Router 12 and the token ring switch 16 also receive the security breach detected frame and perform the same processing operations as defined above for router 14. The bridge 18 receives the security breach detected frame and performs the same processing operations as done by router 14. The managed hub 24 now correlates all of the received filter set frames with the interconnect devices 12, 14, 16, 18 that were discovered via the discovery request/response frames and reenables the port. The managed hub 24 then sends a trap to the management station 26 to indicate that the intruder's port has been reenabled.

As a practical example of the implementation of this invention in a campus LAN environment, FIG. 16 depicts a university setting in which there is a managed hub on each floor of the buildings in a campus network. The network infrastructure consists of a pair of Ethernet switches attached to a campus backbone. Each Ethernet switch is also attached to a plurality of Ethernet managed hubs (one on each floor in each building). The figure shows a student dormitory that is attached to the same network that runs the university administration applications. There are obvious security concerns about students accessing the proprietary administrative information (i.e., grades, transcripts, payroll, accounts receivable/payable, etc.).

An intruder trying to access the network via one of the managed hub ports in the dormitory is stopped at the port of entry to the network and further access to the campus network is prevented by having the intruder's MAC address filtered on all LAN interconnect devices. The symbols containing a "B" in FIG. 16 indicate the points in the campus network where frames with the intruding MAC address are blocked from access to LAN segments by the setting of filters. The data flows corresponding to the example are shown in FIG. 17 and are self-explanatory.

For simplicity, this invention has used the term managed hub to refer to traditional token ring and Ethernet port concentration devices (e.g., IBM 8238, IBM 8224, IBM 8225, IBM 8250, IBM 8260). In reality, the functions of the managed hub can be extended to LAN switches (both token ring and Ethernet) where dedicated stations could be attached directly to the switch port. LAN switches would have to add the functionality of authorizing a set of MAC addresses that could attach to a switch port and detecting any unauthorized accesses to the switch port.

To describe the key aspects of this LAN security invention, it was easiest to illustrate with an implementation using managed hubs. In reality, many large enterprises use a combination of both managed hubs and unmanaged hubs throughout their networks. This invention is readily extendible and the security detection mechanism can easily be integrated into the function of a LAN bridge. The bridge would keep the list of authorized addresses for a given LAN segment where access to the LAN is via low cost unmanaged concentrators. The bridge would then detect any new addresses on the LAN segment and compare the addresses against the authorized list. If an unauthorized address was detected, the bridge would then set up filters for the intruding MAC address, and transmit the security breach detected frame to the other interconnect devices attached to the campus network. In this case, the intruder would be isolated to the LAN segment where the intrusion was first detected. This example shows that the composite function of the managed hub could be integrated into a LAN bridge and the bridge could control the security access for a large segment consisting of unmanaged concentrators.

Another special use of this invention involves the tasks of a network administrator. A key day-to-day task for most network administrators falls into the category of moves, adds, and changes to network configuration. In this invention, the network management station has complete awareness of all of the authorized users throughout the campus network. In the event that a security breach is detected, in the special case where an authorized user is trying to gain access through an unauthorized port, the network management station could detect this situation and automatically take the appropriate actions (i.e., remove filters from the interconnect devices since this is an authorized user). This type of action would assist administrators that work in dynamic environments where there are frequent moves, adds and changes.

The preferred embodiment of the invention has relied upon the detection of unauthorized MAC addresses by the managed hub. It can easily be modified to apply to the network layer (layer 3) or higher layers, in the Open System Interconnection (OSI) protocol stack and work with such well known network protocols as TCP/IP, IPX, HTTP, AppleTalk, DECnet and NETBIOS among others.

Currently, many LAN switches have custom application specific integrated circuits (ASICs) that are designed to detect or recognize frame patterns in hardware. These LAN switches use this frame type recognition capability primarily for frame forwarding based on the IP address and for placing switch ports in a virtual LAN (VLAN). In order to provide security protection at the network layer, it will be clear to one skilled in the art that the authorized address list (AAL) described herein can be extended to include IP addresses. The so-modified AAL, coupled with the LAN switch capability to detect IP addresses in a frame will enable implementation of the detection and prevention phases to support IP addresses. In the detection phase, the ASIC-based LAN switch can be used to obtain the IP address that is connected to a port. The detected IP address would then be compared to the authorized IP addresses in the AAL. If an unauthorized IP address is detected, the invention works as previously described with the disabling of the port and the transmission of the security breach detected frame. In the prevention phase, the interconnect devices are notified of intruding IP addresses and then apply filters for the intruding IP address.

The present invention can also be modified to operate at the application layer (layer 7) of the OSI protocol stack. Currently, several commercially available LAN switches, such as the model 8273 and model 8274 LAN switches available from IBM Corporation, provide a capability for a user-defined policy for creating a VLAN. This user-defined policy enables one to specify an offset into a frame and a value (pattern) to be used to identify the frame. Once the user-defined policy has been defined, the switch ASIC detects all frames matching the specified pattern and places them into a specific VLAN. Since the custom ASIC recognizes the user-defined pattern, it can be programmed to recognize portions of a frame that identify a specific application. This application pattern can then be used as the detection criteria in the invention and thus provide application layer security.

The present invention can be modified further to provide additional security by encryption of the data fields in the frames that are used to implement the inventive concepts described above. One of the most widely known and recognized encryption algorithms is the Data Encryption Standard (DES). The implementation of DES or other encryption algorithm to encrypt the data fields of frames described in this invention can ensure the privacy and integrity of the communication between managed hubs, interconnect devices and network management stations. Security protocols such as Secure Sockets Layer (SSL) utilizing public key encryption techniques are becoming standardized and can be used to further enhance the invention described herein.

While the invention has been particularly shown and described with reference to the particular embodiments thereof, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.

Having thus described our invention, what we claim and desire to secure as Letters Patent is as follows:

1. A method for providing security against intrusion in a computer network having a plurality of managed devices, said method comprising the steps of:

discovering by a first managed device each of said plurality of managed devices that are enabled to provide network security;

detecting an unauthorized address on a first port of said first managed device and disabling said first port;

setting a filter at each of said plurality of managed devices to prevent frames having the unauthorized address from being forwarded through said computer network; and

reenabling said first port after said filtering step has been completed.

2. The method for providing security against intrusion of claim 1 further comprising the step of removing of said filter that had been set at each of said plurality of managed devices.

3. The method for providing security against intrusion of claim 1 wherein said first managed device is a managed hub.

4. The method for providing security against intrusion of claim 1 wherein said first managed device is a switch.

5. The method for providing security against intrusion of claim 1 wherein said plurality of managed devices includes a token ring switch.

6. The method for providing security against intrusion of claim 1 wherein said plurality of managed devices includes an Ethernet switch.

7. The method for providing security against intrusion of claim 1 wherein said plurality of managed devices includes a bridge.

8. The method for providing security against intrusion of claim 1 wherein said plurality of managed devices includes a router.

9. The method for providing security against intrusion of claim 1 wherein said computer network includes a local area network.

10. The method for providing security against intrusion of claim 1 further comprising the steps of building and maintaining an authorized address list at said first managed device of addresses that are allowed to connect to each port in said first managed device.

11. The method for providing security against intrusion of claim 10 wherein each entry in said authorized address list includes a port number and an authorized address.

12. The method for providing security against intrusion of claim 1 wherein said discovering step includes the steps of:

transmitting a discovery request frame by said first managed device, said discovery request frame having a security feature group address;

receiving said discovery request frame at each of said plurality of managed devices and transmitting a discovery response frame back to said first managed device;

building and maintaining an interconnect device list at said first managed device of said plurality of managed devices that transmitted said discovery response frame back to said first managed device.

13. The method for providing security against intrusion of claim 12 wherein each entry in said interconnect device list includes an address of the managed device that sent the discovery response frame and a time stamp extracted from said discovery response frame.

14. The method for providing security against intrusion of claim 11 wherein said detecting step includes the steps of:

comparing, for each port, a source address of a station attempting to connect to said port with the authorized address list of addresses for said port and determining whether said source address is on said authorized address list.

15. The method for providing security against intrusion of claim 12 wherein following said disabling step said method further includes:

sending a trap frame by said first managed device to a network management station indicating that an intrusion has been detected on said first port; and

transmitting a security breach detected frame by said first managed device and having said security feature group address to said plurality of managed devices that have entries in said interconnect device list.

16. The method for providing security against intrusion of claim 15 wherein said security breach detected frame includes a source address of an unauthorized station, the port number of said first managed device at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

17. The method for providing security against intrusion of claim 16 wherein following the receiving of said security breach detected frame and setting of filters, each of said plurality of managed devices performs the additional steps of:

transmitting said security breach detected frame on all ports except the port on which said each managed device received said security breach detected frame;

sending a trap frame to the network management station indicating that said filter has been set as a result of receiving said security breach detected frame; and

transmitting a filter set frame to said first managed device.

18. The method for providing security against intrusion of claim 17 wherein said filter set frame includes the address of said each managed device sending said filter set frame, the source address of said unauthorized station, the port number of said first managed device at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

19. The method for providing security against intrusion of claim 1 wherein following said reenabling step said first managed device sends a trap frame to a network management station indicating that said filtering step has been completed.

20. The method for providing security against intrusion of claim 2 wherein said removing step includes transmitting a security clear condition frame to said plurality of managed devices.

21. The method for providing security against intrusion of claim 2 wherein said removing step includes transmitting a security clear condition frame to a selected managed device of said plurality of managed devices.

22. The method for providing security against intrusion of claim 20 or 21 wherein said security clear condition frame includes said unauthorized address.

23. A system for providing security against intrusion in a computer network having a plurality of managed devices, said system comprising:

means for discovering at a first managed device each of said plurality of managed devices that are enabled to provide network security;

means for detecting an unauthorized address on a first port of said first managed device and means for disabling said first port;

means for setting a filter at each of said plurality of managed devices to prevent frames having the unauthorized address from being forwarded through said computer network; and

means for reenabling said first port of said first managed device after said filtering step has been completed.

24. The system for providing security against intrusion of claim 23 further comprising means at a network management station for generating a security clear condition frame to initiate the removing of said filter that had been set at each of said plurality of managed devices.

25. The system for providing security against intrusion of claim 23 wherein said first managed device is a managed hub.

26. The system for providing security against intrusion of claim 23 wherein said first managed device is a switch.

27. The system for providing security against intrusion of claim 23 wherein said plurality of managed devices includes a token ring switch.

28. The system for providing security against intrusion of claim 23 wherein said plurality of managed devices includes an Ethernet switch.

29. The system for providing security against intrusion of claim 23 wherein said plurality of managed devices includes a bridge.

30. The system for providing security against intrusion of claim 23 wherein said plurality of managed devices includes a router.

31. The system for providing security against intrusion of claim 23 wherein said computer network includes a local area network.

32. The system for providing security against intrusion of claim 23 further comprising means for building and maintaining an authorized address list at said first managed device of addresses that are allowed to connect to each port in said first managed device.

33. The system for providing security against intrusion of claim 32 wherein each entry in said authorized address list includes a port number and an authorized address.

34. The system for providing security against intrusion of claim 23 wherein said means for discovering includes:

means for transmitting a discovery request frame by said first managed device, said discovery request frame having a security feature group address;

means for receiving said discovery request frame at each of said plurality of managed devices and means for transmitting a discovery response frame back to said first managed device;

means for building and maintaining an interconnect device list at said first managed device of said plurality of managed devices that transmitted said discovery response frame back to said first managed device.

35. The system for providing security against intrusion of claim 34 wherein each entry in said interconnect device list includes an address of the managed device that sent the discovery response frame and a time stamp extracted from said discovery response frame.

36. The system for providing security against intrusion of claim 33 wherein said means for detecting includes:

means for comparing, for each port, a source address of a station attempting to connect to said port with the authorized address list of addresses for said port and means for determining whether said source address is on said authorized address list.

37. The system for providing security against intrusion of claim 34 further including:

means for sending a trap frame by said first managed device to a network management station indicating that an intrusion has been detected on said first port; and

means for transmitting a security breach detected frame by said first managed device and having said security feature group address to said plurality of managed devices that have entries in said interconnect device list.

38. The system for providing security against intrusion of claim 37 wherein said security breach detected frame includes a source address of an unauthorized station, the port number of said first managed device at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

39. The system for providing security against intrusion of claim 38 wherein each of said plurality of managed devices further comprises:

means for transmitting said security breach detected frame on all ports except the port on which said each managed device received said security breach detected frame;

means for sending a trap frame to the network management station indicating that said filter has been set as a result of receiving said security breach detected frame; and

means for transmitting a filter set frame to said first managed device.

40. The system for providing security against intrusion of claim 39 wherein said filter set frame includes the address of said each managed device sending said filter set frame, the source address of said unauthorized station, the port number of said first managed device at which the intrusion occurred, and a time stamp representing the time at which the unauthorized station was detected.

41. The system for providing security against intrusion of claim 23 wherein said first managed device further comprises means for sending a trap frame to a network management station indicating that said filter has been set at each of said plurality of managed devices.

42. The system for providing security against intrusion of claim 24 wherein said security clear condition frame includes said unauthorized address.

43. A method for providing security against intrusion in a computer network having a managed hub and at least one interconnect device, said method comprising the steps of:

building and maintaining an authorized address list at said managed hub of addresses that are allowed to connect to each port in said managed hub;

discovering by said managed hub each interconnect device that is enabled to provide network security;

detecting an unauthorized address on a first port of said managed hub and disabling said first port;

setting a filter at each interconnect device to prevent frames having the unauthorized address from being forwarded through said computer network; and

reenabling said first port after said filtering step has been completed.

44. The method for providing security against intrusion of claim 43 further comprising the step of removing of said filter that had been set at each interconnect device.

45. The method for providing security against intrusion of claim 43 wherein said at least one interconnect device includes a token ring switch, an Ethernet switch, a bridge or a router.

46. The method for providing security against intrusion of claim 43 wherein said discovering step includes the steps of:

transmitting a discovery request frame by said managed hub, said discovery request frame having a security feature group address;

receiving said discovery request frame at each interconnect device and transmitting a discovery response frame back to said managed hub;

building and maintaining an interconnect device list at said managed hub of each interconnect device that transmitted said discovery response frame back to said managed hub.

47. The method for providing security against intrusion of claim 46 wherein said detecting step includes the steps of:

comparing, for each port, a source address of a station attempting to connect to said port with an authorized address list of addresses for said port and determining whether said source address is on said authorized address list.

48. The method for providing security against intrusion of claim 46 wherein following said disabling step said method further includes:

sending a trap frame by said managed hub to a network management station indicating that an intrusion has been detected on said first port; and

transmitting a security breach detected frame by said managed hub and having said security feature group address to each interconnect device that has an entry in said interconnect device list.

49. The method for providing security against intrusion of claim 48 wherein following the receiving of said security breach detected frame and setting of filters, each interconnect device performs the additional steps of:

transmitting said security breach detected frame on all ports except the port on which said each interconnect device received said security breach detected frame;

sending a trap frame to the network management station indicating that said filter has been set as a result of receiving said security breach detected frame; and

transmitting a filter set frame to said managed hub.

50. The method for providing security against intrusion of claim 43 wherein following said reenabling step said managed hub sends a trap frame to a network management station indicating that said filtering step has been completed.

51. The method for providing security against intrusion of claim 44 wherein said removing step includes transmitting a security clear condition frame to each interconnect device.

52. A system for providing security against intrusion in a computer network having a managed hub and at least one interconnect device, said system comprising:

means for building and maintaining an authorized address list at said managed hub of addresses that are allowed to connect to each port in said managed hub;

means for discovering by said managed hub each interconnect device that is enabled to provide network security;

means for detecting an unauthorized address on a first port of said managed hub and means for disabling said first port;

means for setting a filter at each interconnect device to prevent frames having the unauthorized address from being forwarded through said computer network; and

means for reenabling said first port of said managed hub after said filtering step has been completed.

53. The system for providing security against intrusion of claim 52 further comprising means at a network management station for generating a security clear condition frame to initiate the removing of said filter that had been set at each interconnect device.

54. The system for providing security against intrusion of claim 52 wherein said at least one interconnect device includes a token ring switch, an Ethernet switch, a bridge or a router.

55. The system for providing security against intrusion of claim 52 wherein said means for discovering includes:

means for transmitting a discovery request frame by said managed hub, said discovery request frame having a security feature group address;

means for receiving said discovery request frame at each interconnect device and means for transmitting a discovery response frame back to said managed hub;

means for building and maintaining an interconnect device list at said managed hub of each interconnect device that transmitted said discovery response frame back to said managed hub.

56. The system for providing security against intrusion of claim **55** wherein said means for detecting includes:

means for comparing, for each port, a source address of a station attempting to connect to said port with an authorized address list of addresses for said port and means for determining whether said source address is on said authorized address list.

57. The system for providing security against intrusion of claim **55** further including:

means for sending a trap frame by said managed hub to a network management station indicating that an intrusion has been detected on said first port; and

means for transmitting a security breach detected frame by said managed hub and having said security feature group address to each interconnect device that has an entry in said interconnect device list.

58. The system for providing security against intrusion of claim **57** wherein each interconnect device further comprises:

means for transmitting said security breach detected frame on all ports except the port on which said each interconnect device received said security breach detected frame;

means for sending a trap frame to the network management station indicating that said filter has been set as a result of receiving said security breach detected frame; and

means for transmitting a filter set frame to said managed hub.

59. The system for providing security against intrusion of claim **52** wherein said managed hub further comprises means for sending a trap frame to a network management station indicating that said filter has been set at each interconnect device.

* * * * *

US005796942A

United States Patent [19]

Esbensen

[11] **Patent Number: 5,796,942**

[45] **Date of Patent: Aug. 18, 1998**

[54] **METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION**

[75] Inventor: **Daniel Esbensen**, Kihei, Hi.

[73] Assignee: **Computer Associates International, Inc.**, Islandia, N.Y.

[21] Appl. No.: **749,352**

[22] Filed: **Nov. 21, 1996**

[51] **Int. Cl.**[6] **G06F 11/00**; G06F 13/00

[52] **U.S. Cl.** **395/187.01**; 395/200.59

[58] **Field of Search** 395/187.01, 186, 395/200.57, 200.58, 200.59; 364/286.4

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,032,979	7/1991	Hecht et al.	395/187.01
5,101,402	3/1992	Chiu et al.	370/17
5,414,833	5/1995	Hershey et al.	395/187.01
5,488,715	1/1996	Wainwright	395/182.02
5,524,238	6/1996	Miller et al.	395/600
5,557,742	9/1996	Smaha et al.	395/186
5,606,668	2/1997	Shwed	395/187.01
5,621,889	4/1997	Lermuzeaux et al.	395/186
5,699,513	12/1997	Feigen et al.	395/187.01

OTHER PUBLICATIONS

Winkler, "A Unix Prototype for Intrusion and Anomaly Detection in Secure Networks", NESC Conference, pp. 1–10, Oct. 1990.

Sebring et al., "Expert System in Intrusion Detection : A Case Study", pp. 74–81.

Debar et al., "A Neural Network Component for an Intrusion Detection System", IEEE, pp. 240–250, 1992.

Dowell et al., "The Computer Watch Data Reduction Tool", pp. 99–108.

Snapp et al., "DIDS(Distributed Intrusion Detection System)–Motivation, Architecture, and Early Prototype", pp. 167–176.

Tener, "Discovery: An Expert System in the Commercial Data Security Environment", pp. 45–53, Computer Security Journal vol. 6, No. 1, Dec. 1986.

Avritzer et al., "Reliability Testing of Rule–Based Systems", IEEE, pp. 1–7, Sep. 1996.

Snapp, "Signature Analysis and Communication Issues in a Distributed Intrusion Detection System", Master Thesis–UCA, pp. 1–40, 1991.

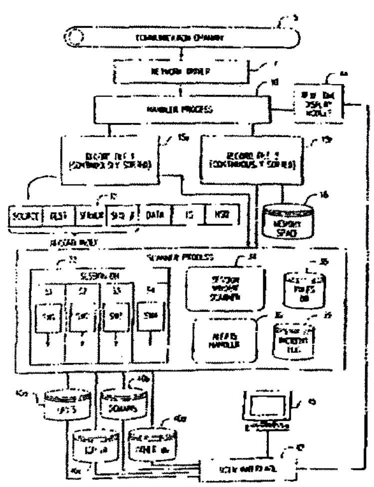
Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Scott T. Baderman
Attorney, Agent, or Firm—Thomas E. O'Connor, Jr.

[57] **ABSTRACT**

A network surveillance system includes a handler process (**10**) for capturing network packets and filtering invalid packets, a first and second continuously sorted record file (**15***a*, **15***b*), and a scanner process (**30**) for scanning all sessions occurring on the network and checking for the presence of certain rules (**38**). When a rule is met, indicating a security incident, a variety of appropriate actions may be taken, including notifying a network security officer via electronic or other mail or recording or terminating a network session. The surveillance system operates completely independently of any other network traffic and the network file server and therefore has no impact on network performance. According to a further embodiment, the invention may include remote surveillance agents (**100***a–c*) for gathering network packets at a remote location and transferring them to a server (**110**) for analysis by a network surveillance system.

20 Claims, 5 Drawing Sheets

Microfiche Appendix Included
(2 Microfiche, 64 Pages)



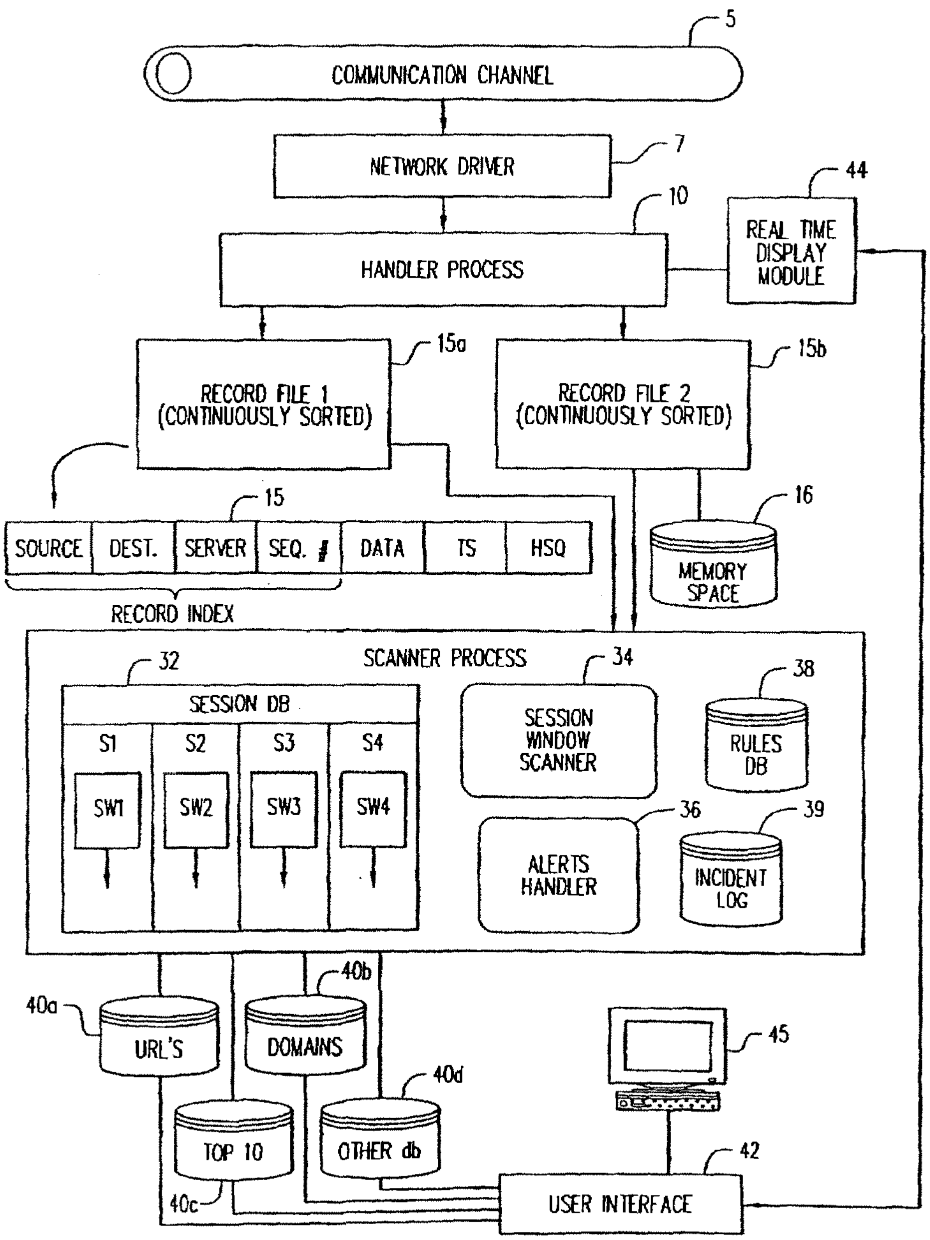

5
COMMUNICATION CHANNEL
NETWORK DRIVER
7
44
10
REAL TIME DISPLAY MODULE
HANDLER PROCESS
15a
15b
RECORD FILE 1 (CONTINUOUSLY SORTED)
RECORD FILE 2 (CONTINUOUSLY SORTED)
15
16
SOURCE
DEST.
SERVER
SEQ. #
DATA
TS
HSQ
MEMORY SPACE
RECORD INDEX
SCANNER PROCESS
32
34
38
SESSION DB
S1
S2
S3
S4
SESSION WINDOW SCANNER
RULES DB
SW1
SW2
SW3
SW4
36
39
ALERTS HANDLER
INCIDENT LOG
40b
40a
URL'S
DOMAINS
45
40d
TOP 10
OTHER db
42
40c
USER INTERFACE

FIG. 1

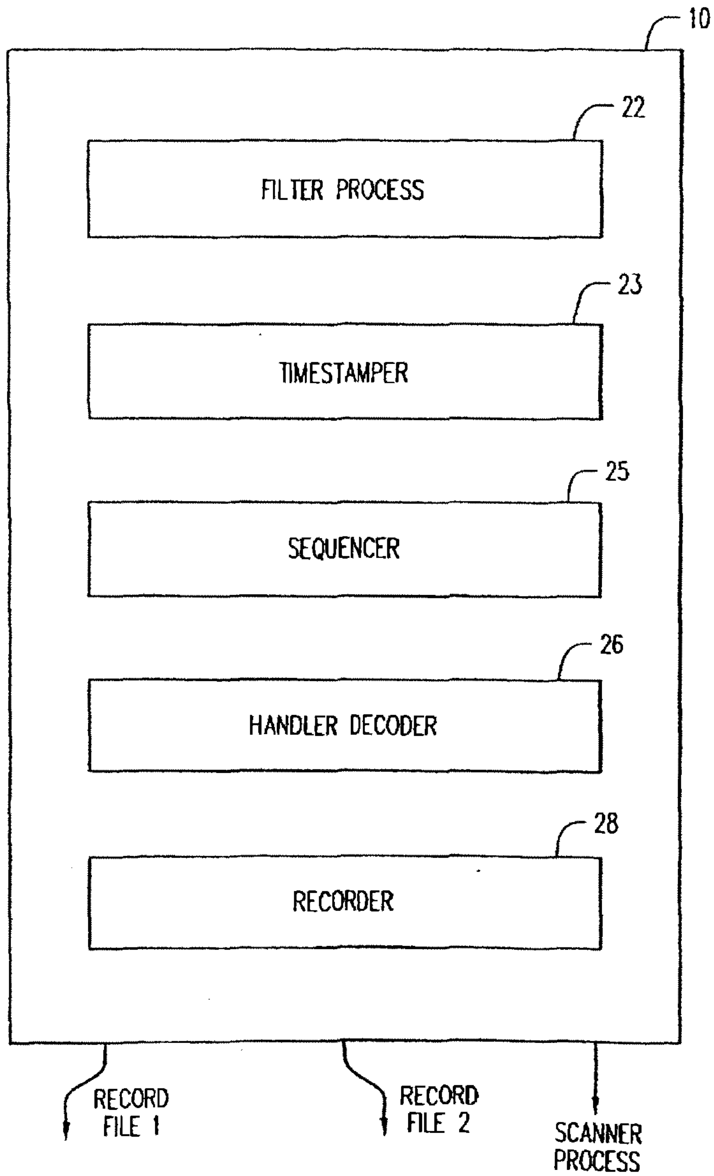

10
22
FILTER PROCESS
23
TIMESTAMPER
25
SEQUENCER
26
HANDLER DECODER
28
RECORDER
RECORD FILE 1
RECORD FILE 2
SCANNER PROCESS

FIG. 2

Electronic Acknowledgement Receipt

EFS ID:	15095555
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	04-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	11:47:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	719862 5dca74a2951d881a06e00962f5f2df4aeab23a67	no	9

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Foreign Reference	C25.pdf	3008098 065807bf4b73a003d18827ca2f8ec6ff33801a92	no	31
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Foreign Reference	C26.pdf	986113 428ec891268fa87080eaaa8cfa7a2ad0d0b28397	no	19
Warnings:					
Information:					
4	Foreign Reference	C27.pdf	8199200 a8fa582ed32622fc0adc879c32cedd5aa6ed289d	no	48
Warnings:					
Information:					
5	Foreign Reference	C28.pdf	1128947 e9375fdfb63581635b68d6263a321db7d4e8aa4b	no	12
Warnings:					
Information:					
6	Non Patent Literature	D1254.pdf	425228 1b734af37f6db3bfa2fbf6717e7151bad0b70d34	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
7	Non Patent Literature	D1255.pdf	574470 3c086015267fe9e1f49f487afd41588bdd654736	no	5
Warnings:					
Information:					
8	Non Patent Literature	D1256.pdf	636843 b6b8ab6df274e68eef427d02fb95bbda25380ec4	no	6
Warnings:					
Information:					
9	Non Patent Literature	D1257.pdf	232366 f6759c8e9c9b23f90a7382e0e3d5b8373da6bae8	no	3

Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	Non Patent Literature	D1258.pdf	572382 1d56e80d0d4ab9cc18915e8bfae50b02e4e3afc2	no	18
Warnings:					
Information:					
11	Non Patent Literature	D1259.pdf	564429 f10d4a399953e5606cb2bc3e6903797b7c2178e2	no	13
Warnings:					
Information:					
12	Non Patent Literature	D1260.pdf	573928 7d171a014e47245cff263cc06a841882716ccada	no	18
Warnings:					
Information:					
13	Non Patent Literature	D1261.pdf	720589 1475f1547e4ccbd2d1a4897f948a13f7a7fcc69f	no	13
Warnings:					
Information:					
14	Non Patent Literature	D1262.pdf	409565 4ee4b0ba0eff1434bb3347ffe0f2bf3744ad0b3f	no	6
Warnings:					
Information:					
15	Non Patent Literature	D1263.pdf	6778779 36d79200c0a10f7c5edf08c16307b9a77a6ed1d8	no	73
Warnings:					
Information:					
16	Non Patent Literature	D1264.pdf	9664167 f5da575d446cdead0d2127f0b614fa2cd8f3f044	no	12
Warnings:					
Information:					
17	Non Patent Literature	D1265part1.pdf	3257426 e10fa16cdf3dcc4c801e3c43b1076cfb845f7222	no	100
Warnings:					
Information:					

18	Non Patent Literature	D1265part2.pdf	4401034 0f6c7db8be993084987583de124a46502cf133b7	no	100
Warnings:					
Information:					
19	Non Patent Literature	D1265part3.pdf	3009164 a79e672b0a35ab1c4061dec70c92ee842790db53	no	100
Warnings:					
Information:					
20	Non Patent Literature	D1265part4.pdf	4214786 01c33769697efb1897305b52fc45d7f8e62bb982	no	100
Warnings:					
Information:					
21	Non Patent Literature	D1265part5.pdf	4113443 a3af25096f2ee9d952c4d9458c6f187d5f1dcff4	no	100
Warnings:					
Information:					
22	Non Patent Literature	D1265part6.pdf	3897956 640a8bf16b4e3192285eb10013a9bda1c349843e	no	100
Warnings:					
Information:					
23	Non Patent Literature	D1265part7.pdf	2164810 343b367b0c48be1264b3e566a452512819d19bb4	no	100
Warnings:					
Information:					
24	Non Patent Literature	D1265part8.pdf	3233153 d368aff43c60b3c2584edf77d5d5e500e020ba56	no	100
Warnings:					
Information:					
25	Non Patent Literature	D1265part9.pdf	2825989 3a267e18a93361908301ce620a7846feaf186d94	no	100
Warnings:					
Information:					
26	Non Patent Literature	D1265part10.pdf	2972212 6f17595814d2d60bf176852f8752c7a359e8cd29	no	100
Warnings:					
Information:					

27	Non Patent Literature	D1265part11.pdf	2160112 4fe7498a9594c1d8647be0d40219460cce69fc81	no	100
Warnings:					
Information:					
28	Non Patent Literature	D1265part12.pdf	3309637 cba2cab7755944754f6f66aedd00edcb01f9be94	no	100
Warnings:					
Information:					
29	Non Patent Literature	D1265part13.pdf	3572344 1838143d07c78fc93a7944f8fbb540f627be2438	no	100
Warnings:					
Information:					
30	Non Patent Literature	D1265part14.pdf	3352910 a9b6228a0fae1c13c1868502f029428c664bf9c0	no	100
Warnings:					
Information:					
31	Non Patent Literature	D1265part15.pdf	3496255 240ee7a5796f70e1f8d6a2691f4a440bd12b3562	no	100
Warnings:					
Information:					
32	Non Patent Literature	D1266.pdf	5201699 0ae584f5461e98ea2eaabd0c81aaac30cd2ed346	no	74
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
33	Non Patent Literature	D1267.pdf	736755 b1992fed98554e4b59532cbba41e8797f215668f	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
34	Non Patent Literature	D1268part1.pdf	9966686 039ca211365c81e14240a28fc3a77ca79908afb8	no	100
Warnings:					
Information:					

35	Non Patent Literature	D1268part2.pdf	8109308 168315ce928ceb4c47339663fa2ff1d375c04d5a	no	100
Warnings:					
Information:					
36	Non Patent Literature	D1268part3.pdf	9980777 fc39c68654853afb3057282101bb3edee29530a7	no	100
Warnings:					
Information:					
37	Non Patent Literature	D1268part4.pdf	9200871 31db4222f327e349cf1bba51e43d4be5bde8461c	no	100
Warnings:					
Information:					
38	Non Patent Literature	D1268part5.pdf	8739047 42e687eab1c4f97e8cdbec4cebe8292574c1a238	no	100
Warnings:					
Information:					
39	Non Patent Literature	D1268part6.pdf	8550043 8980a273a27cf872df5b8a3a8939e6376f4d666b	no	100
Warnings:					
Information:					
40	Non Patent Literature	D1268part7.pdf	8274468 aed7b8b8e6747f3ad646a1eb88c2f4f2ac1afdf2	no	100
Warnings:					
Information:					
41	Non Patent Literature	D1268part8.pdf	7260885 586f6dac84c0958e6fa0692857e7d156886144ec	no	100
Warnings:					
Information:					
42	Non Patent Literature	D1268part9.pdf	8073282 e3ae4bb0871c2747cbf8a35d0daa98d14965a368	no	100
Warnings:					
Information:					
43	Non Patent Literature	D1268part10.pdf	8560232 2009ff8be267bf3dd62fa4a1c385a9c00bff9e5b	no	100
Warnings:					
Information:					

44	Non Patent Literature	D1268part11.pdf	8338473 d9ce938c1efea922374df44140d34e5b5878400c	no	100
Warnings:					
Information:					
45	Non Patent Literature	D1268part12.pdf	5506776 e6982247f8da96c9d0980e9ae459b9c87af5a366	no	70
Warnings:					
Information:					
46	Non Patent Literature	D1269.pdf	8972105 be1666f598735d40a0c5ab28e0d874aefe5ec4c9	no	63
Warnings:					
Information:					
47	Non Patent Literature	D1270.pdf	1203134 b14266da2fa45887796f7084e87e9a1c30781256	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
48	Non Patent Literature	D1271part3.pdf	3504952 bf75da8954442d651d810b504a387458f2e8e525	no	200
Warnings:					
Information:					
49	Non Patent Literature	D1271part4.pdf	3837133 b3916a75633f2c530780acb19ea45f9eb68be34d	no	200
Warnings:					
Information:					
50	Non Patent Literature	D1271part5.pdf	3361641 f9e8b446a2b7e8aee842f3feea04052d569efc15	no	200
Warnings:					
Information:					
51	Non Patent Literature	D1271part6.pdf	2331490 bf576bddb9a97962ac71f7c6d385486f4d390fa4	no	200
Warnings:					
Information:					
52	Non Patent Literature	D1271part7.pdf	2371238 8de6405f301a972e7856fb1b121840007e405650	no	159

Warnings:

Information:

53	Non Patent Literature	_D1272.pdf	9466849 04e0a60844bd23f7253e871fd4b7a6f5f2ba1389	no	78

Warnings:

Information:

54	Non Patent Literature	_D1273.pdf	741623 77b5dd116d906c7a34348098e9a56695e219ccb0	no	12

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

55	Non Patent Literature	D1274.pdf	5328775 4c0a4192f4afc37e4fd00cb14d1873a12fb34d87	no	3

Warnings:

Information:

56	Non Patent Literature	D1275part1.pdf	3706485 2ee9a4f0a2505d16367e2b28156a66167bdfa8f8	no	100

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

57	Non Patent Literature	D1275part2.pdf	3726943 87f5abe5af083c48b57ea8af0289b08d877d194e	no	117

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

58	Non Patent Literature	D1276.pdf	4716307 f483105a7d5d81ac0d42ab25b8e8bab719077221	no	274

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

59	Non Patent Literature	D1271part1.pdf	21132140 b5ac5492ff64fd890a29f5169d35fc0124366b5c	no	200

Warnings:

Information:

60	Non Patent Literature	D1271part2.pdf	4029269 db626da48ada2f728a9a49a060b0f74bb0dc8a4c	no	200

Warnings:

Information:

Total Files Size (in bytes):	270105583

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Acknowledgement Receipt

EFS ID:	15102531
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	04-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	11:51:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1367part17.pdf	2829552 30217a4cf275dc8b68bc609bf783995807a1689f	no	200

Warnings:

Information:

2	Non Patent Literature	D1367part18.pdf	2742291 ca4f5a259b8536daa36b8b9ad409f5a1f1f09a66	no	200
Warnings:					
Information:					
3	Non Patent Literature	D1367part19.pdf	2846638 f69ee9b2ba78513e2b92bd0475d69e6a0fb4abc8	no	200
Warnings:					
Information:					
4	Non Patent Literature	D1367part20.pdf	2598677 de08e1f6b55e257936f24575e7fb5b954f37ee49	no	200
Warnings:					
Information:					
5	Non Patent Literature	D1367part21.pdf	3094007 0e0337954535cbbd5c5f97f2ec0ed5f8b5aa5116	no	200
Warnings:					
Information:					
6	Non Patent Literature	D1367part22.pdf	2473740 bb73365c8ef0c521ea22a11451b039e2c73a2672	no	200
Warnings:					
Information:					
7	Non Patent Literature	D1367part23.pdf	1839430 b40eec3f85e92e6fc9a6665e9f4bbd47672ef115	no	200
Warnings:					
Information:					
8	Non Patent Literature	D1367part24.pdf	2109084 55a0beaf6a686ba1cf800865faf64f519baf0f0b	no	200
Warnings:					
Information:					
9	Non Patent Literature	D1367part25.pdf	2066586 aa9ffa2f6eefa7f5c068f45a8ed0bd414648910a	no	199
Warnings:					
Information:					
10	Non Patent Literature	D1367part26.pdf	7803999 15026aae52ef28e0260fc2f06a4c7aa844abdc29	no	200
Warnings:					
Information:					

11	Non Patent Literature	D1367part27.pdf	6949434 4431b64464736425547db671b1f533059c60ae74	no	200
Warnings:					
Information:					
12	Non Patent Literature	D1367part28.pdf	9420516 99f1bc77d51a1c0e59963be6e8125f62582b2d3b	no	200
Warnings:					
Information:					
13	Non Patent Literature	D1367part29.pdf	8622584 f52e7ff9af96e1be67fa0bf4e415c6edc884d6db	no	200
Warnings:					
Information:					
14	Non Patent Literature	D1367part30.pdf	5691420 aff21f5e3c4226b2942d8ea86909f27b84efeae4	no	200
Warnings:					
Information:					
15	Non Patent Literature	D1367part31.pdf	5147177 79a3fb072f1038c5a54619f42af13855c8d61095	no	200
Warnings:					
Information:					
16	Non Patent Literature	D1367part32.pdf	4989115 ff4eec8f363c85b9e96f09e060f053d2ad486b2a	no	200
Warnings:					
Information:					
17	Non Patent Literature	D1367part33.pdf	5568352 d9e1acef97040cfe5cf0175be4737a18634ccc13	no	200
Warnings:					
Information:					
18	Non Patent Literature	D1367part34.pdf	8490123 3dc07e6085f579298408aa4661548536d76d29a6	no	200
Warnings:					
Information:					
19	Non Patent Literature	D1367part35.pdf	6798116 70e0df0fd8749da37e86e377b2db6d4da47cda6f	no	200
Warnings:					
Information:					

20	Non Patent Literature	D1367part36.pdf	3485165 3eced5d52de48ba1800fe1f8ca4af5138044b82b	no	200
Warnings:					
Information:					
21	Non Patent Literature	D1367part37.pdf	4016005 20e974b5331b980e7d7eb529725eff12e8f04a4f	no	200
Warnings:					
Information:					
22	Non Patent Literature	D1367part38.pdf	3636004 fca83e506ae11779b35e45a8c9cffcfcec7dfca1	no	200
Warnings:					
Information:					
23	Non Patent Literature	D1367part39.pdf	4305786 180e4c71fd02cc5906a2c19341d90b2c86311ce1	no	200
Warnings:					
Information:					
24	Non Patent Literature	D1367part40.pdf	4903541 7f108e007a707311b614e8b6605f08c3ca923ed3	no	200
Warnings:					
Information:					
25	Non Patent Literature	D1367part41.pdf	7138830 72be8053f1ae72eb1cb9bd64705ffa64a059e13a	no	200
Warnings:					
Information:					
26	Non Patent Literature	D1367part42.pdf	9911751 f2070eefb592a0e36d503cc8248a74887ca228b0	no	200
Warnings:					
Information:					
27	Non Patent Literature	D1367part43.pdf	7969144 2f0342bb9b82e4dc238a9f292bce6504fac2fdfa	no	200
Warnings:					
Information:					
28	Non Patent Literature	D1367part44.pdf	9714518 69809f99901efd296a487fec6c8953e1e9fb5dbe	no	200
Warnings:					
Information:					

29	Non Patent Literature	D1367part45.pdf	9464624 0e72b0765bd452396169aed99d9a7db2f50f713a	no	200
Warnings:					
Information:					
30	Non Patent Literature	D1367part46.pdf	8840128 ec4819ce60039eeb925758cc05992220baa447cc	no	200
Warnings:					
Information:					
31	Non Patent Literature	D1367part47.pdf	7390404 20f6a873451180115e534ea00e5c96c90989a25b	no	200
Warnings:					
Information:					
32	Non Patent Literature	D1367part48.pdf	5183735 9fe8a56297a63015b48d8fc8f90ea07a06fe0c6e	no	200
Warnings:					
Information:					
33	Non Patent Literature	D1367part49.pdf	6393126 97f0f2fb7616056656bf05eb3b815ac0ade60d84	no	200
Warnings:					
Information:					
34	Non Patent Literature	D1367part50.pdf	6962577 de042b7abfe7a3823a7502a00854afdeb35de8fb	no	199
Warnings:					
Information:					
35	Non Patent Literature	D1367part51.pdf	6443871 86bdf9113d5cb529d8335a5af2a258fda7ec218a	no	200
Warnings:					
Information:					
36	Non Patent Literature	D1367part52.pdf	6068436 a0c2088b834a5b132fd59e9003d97da81379d02a	no	200
Warnings:					
Information:					
37	Non Patent Literature	D1367part53.pdf	6570870 9600469d0807f84cf8dcb941dbc5f49906102a72	no	200
Warnings:					
Information:					

38	Non Patent Literature	D1367part54.pdf	4949670 4da01fa51501b8e45d981619e0d3b0e3e5c462f7	no	200
Warnings:					
Information:					
39	Non Patent Literature	D1367part55.pdf	4695155 12e5f7564ceabb745e9126103bb9ec7f09675e79	no	200
Warnings:					
Information:					
40	Non Patent Literature	D1367part56.pdf	4957213 8e4df5a225d7b4bd4f869b2dece14d8e6a2e31bf	no	200
Warnings:					
Information:					
41	Non Patent Literature	D1367part57.pdf	8708817 70e6f68114bea0dcb0ecee736a1bb7dfb121a188	no	200
Warnings:					
Information:					
42	Non Patent Literature	D1367part58.pdf	6779256 ed3b9e77755c9ad2e0442bf013062a284ae4f722	no	200
Warnings:					
Information:					
43	Non Patent Literature	D1367part59.pdf	5328626 36f13527af4c3ff03ecdfb50c9414156531caa1f	no	200
Warnings:					
Information:					
44	Non Patent Literature	D1367part60.pdf	6773524 7d88e8851457b6ec52c0e506743776308e8cfab3	no	200
Warnings:					
Information:					
45	Non Patent Literature	D1367part61.pdf	6755777 d86235569ce34aab55a7ba3b1cfb3eeedbc5d895	no	200
Warnings:					
Information:					
46	Non Patent Literature	D1367part62.pdf	6058621 fdb98d4cd4a610bc5206ddea9b870c9c2f63b03d	no	200
Warnings:					
Information:					

47	Non Patent Literature	D1367part63.pdf	5968372 58c23cf102e013185469ea1768e1fb40df7c07c3	no	200
Warnings:					
Information:					
48	Non Patent Literature	D1367part64.pdf	5493823 76fa05ded24ff89bf3dc542c2a8e062ff32eb19a	no	200
Warnings:					
Information:					
49	Non Patent Literature	D1367part65.pdf	8929581 498f89623b235dfff910de52c69e435a4339a8ce	no	200
Warnings:					
Information:					
50	Non Patent Literature	D1367part66.pdf	8355250 e70796817e7f1ace3a8bd94ad48f83e06ad3571f	no	200
Warnings:					
Information:					
51	Non Patent Literature	D1367part67.pdf	6039483 313887801f0db75273c9f17ebcbb4857770ad0fa	no	200
Warnings:					
Information:					
52	Non Patent Literature	D1367part68.pdf	4701060 76c54663b19e4cdc6de528e1d02526310d99f594	no	200
Warnings:					
Information:					
53	Non Patent Literature	D1367part69.pdf	5677709 bf9092148071fa016dd283e4653d16387d207e3f	no	200
Warnings:					
Information:					
54	Non Patent Literature	D1367part70.pdf	5346438 b0bdb5bf643c66a6c547b118acbde76e5c2fafd1	no	200
Warnings:					
Information:					
55	Non Patent Literature	D1367part71.pdf	6946216 83161ad44c5a2afabed818c4c84a7478dd13ccbf	no	200
Warnings:					
Information:					

56	Non Patent Literature	D1367part72.pdf	5859323 d34bd2e2f0b1d4c250f9f1e66208227fed296bae	no	200
Warnings:					
Information:					
57	Non Patent Literature	D1367part73.pdf	6310488 acaa235876d1179a8cab197e868278103e8a6974	no	200
Warnings:					
Information:					
58	Non Patent Literature	D1367part74.pdf	9839138 5fa9f7bce783d1983da23c8f76aa161503d47140	no	200
Warnings:					
Information:					
59	Non Patent Literature	D1367part75.pdf	11273482 d1aabce64442d1b48834bedcdf8f4fb1cf195d91	no	199
Warnings:					
Information:					
60	Non Patent Literature	D1367part76.pdf	7216090 93fbd52354a7f9e43d0870b497cd80fe70513685	no	200
Warnings:					
Information:					
			Total Files Size (in bytes):	363442468	

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Electronic Acknowledgement Receipt

EFS ID:	15102291
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	04-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	11:50:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1336.pdf	6224382 5532df0a9705e937962cef6757fb66839f4567d9	no	207

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
2	Non Patent Literature	D1337.pdf	1693967 86bc65b9e9ce85091006dfde1b751d20d77db78b	no	4
Warnings:					
Information:					
3	Non Patent Literature	D1338.pdf	1010871 8cd58e8c9a621ebb661db8c15d35495c3eced84c	no	1
Warnings:					
Information:					
4	Non Patent Literature	D1339.pdf	1361716 76ae31ebed6a611e46ac7fd2fc480fa1c01043dc	no	4
Warnings:					
Information:					
5	Non Patent Literature	D1340.pdf	117551 9f3ccab33733fb8b4c91aeb24869af4887933b5e	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:					
6	Non Patent Literature	D1341.pdf	1586481 18c999d527a6e63e49a24243eb2848bba71e3cbb	no	2
Warnings:					
Information:					
7	Non Patent Literature	D1342.pdf	4567422 33c7c83c8facdf6b1925227a9df809c2f45f5d14	no	39
Warnings:					
Information:					
8	Non Patent Literature	D1343.pdf	1386522 fc6a4547b1e56c6f6ed6d1d9133e1dff81009fbf	no	128
Warnings:					
Information:					
9	Non Patent Literature	D1344.pdf	3224028 143baeeedb8e7fc279fc796714845fc22ce83bc1	no	27
Warnings:					
Information:					

10	Non Patent Literature	D1345part1.pdf	8057998 f47dae52b5279e5071879b2230170c2d849dcbd3	no	100
Warnings:					
Information:					
11	Non Patent Literature	D1345part2.pdf	7593970 5b5c0726510c37610f7563687de708e4389bb895	no	100
Warnings:					
Information:					
12	Non Patent Literature	D1345part3.pdf	9257367 9e07a4f4e2e1e05ec1172bd0dfa7083598da7e71	no	150
Warnings:					
Information:					
13	Non Patent Literature	D1345part4.pdf	10336191 1c01b8ccdec738f5c0c088bfc2b0cf22ad1f131a	no	150
Warnings:					
Information:					
14	Non Patent Literature	D1345part5.pdf	8946138 f05004993463461699993af6370a7710d0d9cb30d	no	150
Warnings:					
Information:					
15	Non Patent Literature	D1345part6.pdf	8828613 099ca1650d1b9f5b7c2459058c6346b1d111d55e	no	150
Warnings:					
Information:					
16	Non Patent Literature	D1345part7.pdf	8560141 e6bd414516d47087f599aab3f308622e8283df52	no	150
Warnings:					
Information:					
17	Non Patent Literature	D1345part8.pdf	9356808 af3313861cd5f9b729d178896b769ed4455f4162	no	150
Warnings:					
Information:					
18	Non Patent Literature	D1345part9.pdf	9764625 64b894c3184974d20bebd232d095bb54bd010a6b	no	150
Warnings:					
Information:					

19	Non Patent Literature	D1345part10.pdf	1423238 596a082b8447685e7dfd212ffde96e40bcebc406	no	150
Warnings:					
Information:					
20	Non Patent Literature	D1346.pdf	1919004 a749b23be1d527cdca70d02fdf7ec267c9b48f7c	no	3
Warnings:					
Information:					
21	Non Patent Literature	D1347.pdf	1497286 5782c123c01822cd82847467cc58c1549d2893d4	no	3
Warnings:					
Information:					
22	Non Patent Literature	D1348.pdf	3063828 e518be7623faedbcec17d1bb276de1240aa5b5c2	no	36
Warnings:					
Information:					
23	Non Patent Literature	D1349.PDF	1286364 958865142a880cea138f87b5c810c0f1df4fc639	no	4
Warnings:					
Information:					
24	Non Patent Literature	D1350.pdf	1315534 15e30298a1660e16fb614885f43a9935befda828	no	3
Warnings:					
Information:					
25	Non Patent Literature	D1351.pdf	3078803 a08178b7efe18b87b23e63f3d061cc3e44699c99	no	22
Warnings:					
Information:					
26	Non Patent Literature	D1352.pdf	7439047 d9da5167524e9d452a1feccd1bede7f2d4c483f3	no	116
Warnings:					
Information:					
27	Non Patent Literature	D1353.pdf	739926 b3492a5af9e4cd344c7af5263b9f55ac4fb6e4c6	no	6
Warnings:					
Information:					

28	Non Patent Literature	D1354.pdf	139202 a1a19c125aa4b950132854f4c88d98a1550cc064	no	68
Warnings:					
Information:					
29	Non Patent Literature	D1355.pdf	1862178 10c4110f046b1dc6bae52b1113396432015cf1f7	no	10
Warnings:					
Information:					
30	Non Patent Literature	D1356.pdf	1878558 ccd50a0a173c9affbe903665d792c92a3747785a	no	30
Warnings:					
Information:					
31	Non Patent Literature	_D1357part1.pdf	5635560 369fd43e1b747710fe7c672a31393d3fd4e24d38	no	75
Warnings:					
Information:					
32	Non Patent Literature	_D1357part2.pdf	6501605 14d71a85aee6813de8571fbca2b7f9dbf3341fe9	no	75
Warnings:					
Information:					
33	Non Patent Literature	_D1357part3.pdf	6588852 f01f67f9e3ef2989c0c018db7f3bb7e038341c1b	no	75
Warnings:					
Information:					
34	Non Patent Literature	_D1357part4.pdf	6656277 240dbe444a97bc7865b5a1fae3ec74b373b353ae	no	75
Warnings:					
Information:					
35	Non Patent Literature	_D1357part5.pdf	5013231 0731e95beb06dc8e1dad1d205b33d80def795971	no	56
Warnings:					
Information:					
36	Non Patent Literature	D1358.pdf	1459176 09af3d6fa978700a4183ee42d3defabc8dc0c6fd	no	9
Warnings:					
Information:					

37	Non Patent Literature	D1359.pdf	53296 9613954f4f62b572a41c199011e31d85da45bd65	no	5
Warnings:					
Information:					
38	Non Patent Literature	D1360.pdf	2039339 fa1e4f7f58a54caaf7839afd2e2ea65a0731ed52	no	8
Warnings:					
Information:					
39	Non Patent Literature	D1361.pdf	618909 e511497cba6683792a8519d5a04ac45bb1461166	no	5
Warnings:					
Information:					
40	Non Patent Literature	D1362.pdf	373586 22c4361dfd74c3b6fa4eea0d570fc87e8212e37c	no	3
Warnings:					
Information:					
41	Non Patent Literature	D1363.pdf	686232 08fc3a5de12cee958594ad4dc03e1b8c883c72ad	no	6
Warnings:					
Information:					
42	Non Patent Literature	D1364.pdf	83229 7f8cb9e409de8c4514fd60a5389d27355b89a7d8	no	1
Warnings:					
Information:					
43	Non Patent Literature	D1365.pdf	55043 5d7dc77c413956d0fdad7ea3c1680d1777c49e59	no	17
Warnings:					
Information:					
44	Non Patent Literature	D1366.pdf	2675465 faa218677b0b25f03b26af98f7e0f1feb868e360	no	11
Warnings:					
Information:					
45	Non Patent Literature	D1367part1.pdf	15960835 fe4eac6ef853165892de444e6b46f9c8b2941991	no	201
Warnings:					
Information:					

46	Non Patent Literature	D1367part2.pdf	3171465 d41604ab63c8e5aaac499ffead29d43cbeb1f4ae	no	200
Warnings:					
Information:					
47	Non Patent Literature	D1367part3.pdf	3067154 eb4e223c50a6efb9b76ad963ca690fc0e148a696	no	200
Warnings:					
Information:					
48	Non Patent Literature	D1367part4.pdf	2754394 27542e3bfcef4163e8eaf027c3f59b3522719945	no	200
Warnings:					
Information:					
49	Non Patent Literature	D1367part5.pdf	3204769 b84f42ec4c8b3735e9e1d10456b0a4239b698cf5	no	200
Warnings:					
Information:					
50	Non Patent Literature	D1367part6.pdf	3562036 b5ea9c4993f34b249ce1de35548d1a328853a064	no	200
Warnings:					
Information:					
51	Non Patent Literature	D1367part7.pdf	3193057 2f0b7e75e2d4676116207937450bd355799f6882	no	200
Warnings:					
Information:					
52	Non Patent Literature	D1367part8.pdf	1736291 5c12f84a88ac4f0b839ca6d18800ccaa2ed770b3	no	200
Warnings:					
Information:					
53	Non Patent Literature	D1367part9.pdf	2778626 997661c418a9b95eb9fd80feb03c6537e59b2ea2	no	200
Warnings:					
Information:					
54	Non Patent Literature	D1367part10.pdf	2220634 136cee2ab62a09694855b9e5026450a12dc45ebf	no	200
Warnings:					
Information:					

55	Non Patent Literature	D1367part11.pdf	2896543 ccfb4ec5c7678f0697fad134148b0a51ef69ec5c	no	200
Warnings:					
Information:					
56	Non Patent Literature	D1367part12.pdf	3275415 54a76826c8a38b1d8d69ba5ca6b12edb294deee3	no	200
Warnings:					
Information:					
57	Non Patent Literature	D1367part13.pdf	2574446 1540300550e6afb5ffabffd0b1702c7bcc47e835	no	200
Warnings:					
Information:					
58	Non Patent Literature	D1367part14.pdf	2870775 33427066647a8efc1b58131ff552d2d39f6cf66c	no	200
Warnings:					
Information:					
59	Non Patent Literature	D1367part15.pdf	3533177 ce6ef0c77a5b674f2eb7a16d8c0b405f4ea9cf3d	no	200
Warnings:					
Information:					
60	Non Patent Literature	D1367part16.pdf	3786071 9784e33a377b4c0ed3296f46a47d237535a4b80f	no	200
Warnings:					
Information:					
			Total Files Size (in bytes):	226543247	

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:	13339257
Filing Date:	28-Dec-2011
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kerrie Jones
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

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

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

Electronic Acknowledgement Receipt

EFS ID:	15106995
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	04-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	14:53:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	1579
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Fee Worksheet (SB06)	fee-info.pdf	30674 e7649fc6d476eb03cf73bc6bbbb8f31edb4a2dcb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	30674		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				Complete if Known	
				Application Number	13/339,257
				Filing Date	12-28-2011
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	77580-154(VRNK-1CP3CNFT4)

CERTIFICATION STATEMENT

This Information Disclosure Statement is being filed after the receipt of the final office action dated December 10, 2012.

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement; **Cited reference A167 cited by examiner in office action dated March 20, 2013 for U.S. patent application number 13/617,375; Cited references A168, A169 and B22 cited by examiner in office action dated December 14, 2010 for U.S. patent application number:11/839,937**

.

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby H. Kusmer

Date: 3/26/13

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

DM_US 41676297-1.077580.0154

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

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
	A167	6,182,227	01-30-2001	Blair et al.	
	A168	5,838,796	11/17/1998	Mittenthal	
	A169	4,677,434	06/30/1987	Fascenda	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B22	US2002/0002675	01/03/2002	Bush	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

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.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal

Application Number:	13339257
Filing Date:	28-Dec-2011
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kerrie Jones
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

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

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

Electronic Acknowledgement Receipt

EFS ID:	15355379
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	26-MAR-2013
Filing Date:	28-DEC-2011
Time Stamp:	14:55:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	1314
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Information Disclosure Statement (IDS) Form (SB08)	0154IDS.pdf	124181 bac283f0b9f29dccebb9ca5fc03748726cee06f6	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Fee Worksheet (SB06)	fee-info.pdf	30678 c8269f3b170669cd7b9c42d508a0a2ed9ae9b12d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	154859		

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

23630 7590 05/16/2013

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

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

DATE MAILED: 05/16/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	12/28/2011	Victor Larson	77580-154(VRNK-1CP3CNFT4)	1084

TITLE OF INVENTION: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$0	$0	$1780	08/16/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: <u>Mail</u> **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or <u>Fax</u> (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23630 7590 05/16/2013

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

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	12/28/2011	Victor Larson	77580-154(VRNK-1CP3CNFT4)	1084

TITLE OF INVENTION: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$0	$0	$1780	08/16/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LIM, KRISNA	2453	709-204000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
   (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
   1 ______________________________
   2 ______________________________
   3 ______________________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies ______________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____________ (enclose an extra copy of this form).

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
❑ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
❑ Applicant changing to regular undiscounted fee status.	NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature ____ Date ____

Typed or printed name ____ Registration No. ________________________________

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	12/28/2011	Victor Larson	77580-154(VRNK-1CP3CNFT4)	1084

23630 7590 05/16/2013

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

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

DATE MAILED: 05/16/2013

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

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 13/339,257	Applicant(s) LARSON ET AL.	
	Examiner KRISNA LIM	Art Unit 2453	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment filed 02/27/2013*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-9, 11-23 and 25-32*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. ______ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

   Interim copies:

   a) ☐ All b) ☐ Some c) ☐ None of the: Interim copies of the priority documents have been received.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)
1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Krisna Lim/
Primary Examiner, Art Unit 2453

Pursuant to 37 C.F.R 1.109 and M.P.E.P 1302.14, the following is an Examiner's Statement of Reasons for Allowance:

Kiuchi discloses that the C-HTTP name server stores the IP address and public key of a particular computer in a data structure that maps the name of the particular computer to the corresponding IP address and public key. Kiuchi discloses that the client-side proxy sends a request to the C-HTTP, where the request is asking the C-HTTP server for permission to establish a connection with a server-side proxy.

Wesinger describes a system in which a configuration file is stored on a series of firewalls. The configuration files store security information by domain name and use the domain name to determine if a particular request is to be allowed.

Moreover, Wesinger discloses the following sequence: (i) a request is received by the firewall/DNS server, (ii) the domain name in the request is looked up in the configuration file, (iii) if the connection is allowed, then the firewall/DNS server may invoke code that performs channel processing, which includes encryption.

Wesinger discloses that DNS propagation happens in a normal manner, but also teaches that the DNS propagation happens through the firewall servers, and the DNS propagation is subject to the allow or deny connection rules.

In Examiner's opinion, both Kiuchi and Wesinger **may not clearly** disclose the feature of "*intercepting a request to look up an IP address based on a domain name* of a secure web site (i.e., the second network device) and determining whether or not to establish a secure communication connection". Moreover, in Examiner's opinion, Examiner believes that the requested is intercepted and determined before the request reached the firewall/DNS server.

Examiner considers the applicants' claims 1-9, 11-23 and 25-32 to be allowable based on the claim interpretation and Examiner's opinion based on Examiner's understanding during the personal interview with Inventor Robert Short on October 11,

2012. Thus, **Examiner's opinion should not be imputed to the concession of the prior arts and the exhaustion of the prior arts for determining the patentability of any or all claims**.

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956. The examiner can normally be reached on Tuesday to Friday from 7:10 AM to 5:40 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele, can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

Kl
May 3, 2013

/Krisna Lim/
Primary Examiner, Art Unit 2453

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

This Information Disclosure Statement is being filed after the receipt of the final office action dated December 10, 2012.

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement; **Cited reference A167 cited by examiner in office action dated March 20, 2013 for U.S. patent application number 13/617,375; Cited references A168, A169 and B22 cited by examiner in office action dated December 14, 2010 for U.S. patent application number:11/839,937**

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

Toby Kusmer

Date: 3/26/13

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

DM_US 41676297-1.077580.0154

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

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
	A167	6,182,227	01-30-2001	Blair et al.	
	A168	5,838,796	11/17/1998	Mittenthal	
	A169	4,677,434	06/30/1987	Fascenda	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B22	US2002/0002675	01/03/2002	Bush	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

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.	

EXAMINER /Krisna Lim/	DATE CONSIDERED 05/03/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Issue Classification	**Application/Control No.** 13339257	**Applicant(s)/Patent Under Reexamination** LARSON ET AL.
	Examiner KRISNA LIM	**Art Unit** 2453

CPC

Symbol				Type	Version
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		

CPC Combination Sets

Symbol				Type	Set	Ranking	Version
			/				
			/				

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
709	227	G	0	6	F	15 / 16 (2006.01.01)						

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 30	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 05/03/2013 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Issue Classification	**Application/Control No.** 13339257	**Applicant(s)/Patent Under Reexamination** LARSON ET AL.
	Examiner KRISNA LIM	**Art Unit** 2453

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 30	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 (Primary Examiner)	05/03/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

U.S. Patent and Trademark Office

Part of Paper No. 20130503

Issue Classification	Application/Control No. 13339257	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 2453

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6	22	22												
7	7	23	23												
8	8		24												
9	9	25	25												
	10	26	26												
11	11	27	27												
12	12	28	28												
13	13	10	29												
14	14	29	30												
16	15	15	31												
24	16	30	32												

NONE (Assistant Examiner)	(Date)	Total Claims Allowed: 30	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 (Primary Examiner)	05/03/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Search Notes	**Application/Control No.** 13339257	**Applicant(s)/Patent Under Reexamination** LARSON ET AL.
	Examiner KRISNA LIM	**Art Unit** 2453

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
709	223-227	02/23/2012	kl
	updated above	07/18/2012	kl
709	223-227	05/03/2013	kl

SEARCH NOTES

Search Notes	Date	Examiner
East, Inventors	02/23/2012	kl
Inventors, Prior Arts submitted by applicants	05/03/2013	kl

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
709	227	05/03/2013	kl

Index of Claims	Application/Control No. 13339257	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	02/25/2012	07/18/2012	12/01/2012	05/03/2013					
1	1	✓	✓	✓	=					
2	2	✓	✓	✓	=					
3	3	✓	✓	✓	=					
4	4	✓	✓	✓	=					
5	5	✓	✓	✓	=					
6	6	✓	✓	✓	=					
7	7	✓	✓	✓	=					
8	8	✓	✓	✓	=					
9	9	✓	✓	✓	=					
	10	✓	✓	✓	=					
11	11	✓	✓	✓	-					
12	12	✓	✓	✓	=					
13	13	✓	✓	✓	=					
14	14	✓	✓	✓	=					
16	15	✓	✓	✓	=					
24	16	✓	✓	✓	=					
17	17	✓	✓	✓	=					
18	18	✓	✓	✓	=					
19	19	✓	✓	✓	=					
20	20	✓	✓	✓	=					
21	21	✓	✓	✓	=					
22	22	✓	✓	✓	=					
23	23	✓	✓	✓	=					
	24	✓	✓	✓	-					
25	25	✓	✓	✓	=					
26	26	✓	✓	✓	=					
27	27	✓	✓	✓	=					
28	28	✓	✓	✓	=					
10	29				=					
29	30				=					
15	31				=					
30	32				=					

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A163	5,007,051	04/09/1991	Dolkas et al.	
	A164	5,345,439	09/06/1994	Marston	
	A165	5,884,038	03/16/1999	Kapoor	
	A166	6,266,699	07/24/2001	Sevcik	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	C25	JP 09-270803	10/14/1997	Furukawa Electric Co. Ltd.		English Abstract	
	C26	JP 10-111848	04/28/1998	AT&T Corp.		English Abstract	
	C27	JP 10-215244	08/11/1998	Sony Corp.		English Abstract	
	C28	JP 04-117826	04/17/1992	Matsushita Electric Ind. Co. 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.	
	D1254	Eastlake, "Domain Name System Security Extensions," Network Working Group, RFC: 2535 pages 2-11 (March 1999)	
	D1255	Press Release; VirnetX and Aastra Sign a Patent License Agreement, 4 pages, May 2012, Printed from Website: http://virnetx.com/virnetx-and-aastra-sign-a-patent-license-agreement/	
	D1256	Press Release; VirnetX and Mitel Networks Corporation Sign a Patent License Agreement, 5 pages, July 2012, Printed from Website: http://virnetx.com/virnetx-and-mitel-networks-corporation-sign-a-patent-license-agreement/	
	D1257	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/vimetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1258	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001789 pp. 1-18, dated December 20, 2012	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1259	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001851 pp. 1-13, dated December 30, 2012	
	D1260	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001788 pp. 1-18, dated December 18, 2012	
	D1261	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001856 pp. 1-13, dated December 30, 2012	
	D1262	VirnetX vs Apple Transcript of Trial, Afternoon Session, 12:05 p.m., dated November 5, 2012	
	D1263	Certified Copy dated September 18, 2012 of U.S. Patent Number 6,502,135, 73 pages	
	D1264	Certified Copy dated December 30, 2009 of Assignment for Patent Application Number 95/047,83 12 pages	
	D1265	Certified Copy dated March 11, 2008 of Patent Application Number 09/504,783, 1500 pages	
	D1266	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,418,504, 74 pages	
	D1267	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number: 10/714,849, 10 pages	
	D1268	Certified Copy dated April 4, 2011 of Patent Application Number 10/714,849, 1170 pages	
	D1269	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,490,151, 63 pages	
	D1270	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number 10/259,494, 19 pages	
	D1271	Certified Copy dated April 4, 2011 of Application Number 10/259,454, 1359 pages	
	D1272	Certified Copy dated April 12, 2011 of U.S. Patent Number 7,921,211, 78 pages	
	D1273	Certified Copy dated October 17, 2012 of Assignment for Application Number 11/840,560, 12 pages	
	D1274	Certified Copy dated April 20, 2011 of Application Number 11/840,560, 3 pages	
	D1275	iPhone User Guide for iPhone OS 3.1 Software, 217 pages, 2009	
	D1276	iPhone User Guide for iOS 4.2 and 4.3 Software, 274 pages, 2011	
	D1277	iPhone User Guide for iPhone and iPhone 3G, 154 pages, 2008	
	D1278	iPhone User Guide for iOS 5.0 Software, 163 pages, 2011	
	D1279	iPad User Guide for iOS 5.0 Software, 141 pages, 2011	
	D1280	iPad User Guide for iOS 4.2 Software, 181 pages, 2010	
	D1281	iPad User Guide for iOS 4.3 Software, 198 pages, 2011	
	D1282	iPad User Guide, 154 pages, 2010	
	D1283	iPod Touch User Guide for iOS 5.0 Software, 143 pages, 2011	
	D1284	iPod Touch User Guide, 122 pages, 2008	
	D1285	iPod Touch User Guide for iPhone OS 3.0 Software, 153 pages, 2009	
	D1286	iPod Touch User Guide for iPhone OS 3.1 Software, 169 pages, 2009	
	D1287	iPod Touch User Guide for iOS 4.3 Software, 230 pages, 2011	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1288	iPod Touch Features Guide, 98 pages, 2008	
	D1289	VPN Server Configuration for iOS; Networking & Internet Enterprise Deployment, 12 pages, 2011	
	D1290	iPhone Configuration Utility User Guide, 26 pages, 2010	
	D1291	iPhone Configuration Utility; Networking & Internet: Enterprise Deployment, 26 pages, 2011	
	D1292	iPhone Configuration Utility; Networking>Internet & Web, 24 pages, 2010	
	D1293	iOS Configuration Profile Reference; Networking & Internet: Enterprise Deployment, 24 pages, 2011	
	D1294	iPhone OS Enterprise Deployment Guide; Second Edition, for Version 3.1 or Later, 91 pages, 2009	
	D1295	iPhone OS; Enterprise Deployment Guide; Second Edition, for Version 3.2 or Later, 90 pages, 2010	
	D1296	CFHost Reference; Developer, 20 pages, 2008	
	D1297	CFNetwork Programming Guide; Developer, 60 pages, 2011	
	D1298	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1299	Mac OS X Devloper Library; CFHostSample.c, 1 page (no date provided)	
	D1300	Mac OS X Developer Library; CFHostSample, 1 page, 2004	
	D1301	Mac OS X Developer Library; Document Revision History, 1 page, 2004	
	D1302	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1303	Apple Push Notification Service; Distribution Service, Version 1.0, 6 pages, 2009	
	D1304	iOS Human Interface Guidelines; Developer, 184 pages, 2012	
	D1305	Networking & Internet Starting Point, 3 pages, 2011	
	D1306	Server Admin. 10.5 Help; Viewing a VPN Overview, 1 page (no date provided)	
	D1307	iOS: Supported Protocols for VPN, 2 pages, 2010	
	D1308	IPhone in Business Virtual Private Networks (VPN), 3 pages, 2010	
	D1309	iPhone and iPad in Business Deployment Scenarios, 26 pages, 2011	
	D1310	Deploying iPhone and iPad Virtual Private Networks, 3 pages, 2011	
	D1311	Deploying iPhone and iPad; Security Overview, 6 pages, 2011	
	D1312	Pad in Business; "Ready for Work," 2012, 5 pages	
	D1313	iOS: Using FaceTime, 2 pages, 2011, Printed from website http://support.apple.com/kb/HT4317	
	D1314	MobileMe: "Secure Chat" is Unavailable in OS X Lion, 2 pages, 2012, Printed from Website: http://support.apple.com/kb/TS3902	
	D1315	iPhone 4 and iPod Touch (4th Generation): Using FaceTime, 2 pages, 2010, Printed from Website: http://support.apple.com/kb/HT4319	
	D1316	IPhone; "Picking Up Where Amazing Left Off," 11 pages, 2012, Printed from Website: http://www.apple.com/iPhone/features/facetime	
	D1317	FaceTime for Mac; "Say Hello to FaceTime for Mac," 4 pages, 2012, Printed from Website: http://www.apple.com/mac/facetime	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1318	iPad; "Your New Favorite Way to do Just About Everything," 8 pages, 2012, Printed from Website" http://www.apple.com/ipad/built-in-apps/	
	D1319	iPod Touch; FaceTime, "Oh, I see what you're saying," 2 pages (no date provided)	
	D1320	Apple Press Info; Apple Presents iPhone 4, Printed from Website: http://www.apple.com/pr/library/apple-presents-iphone (no date)	
	D1321	iPod Touch; FaceTime, "Oh I See What You're Saying,", 3 pages, 2012, Printed from Website: http://www.apple.com/iPodtouch/built-in-apps/facetime.htm	
	D1322	IOS 4, The World's Most Advanced Mobile Operating System, 5 pages, Printed from Website: http://www.apple.com/iphone/ios4 (no date provided)	
	D1323	Apple Press Info; Apple Reinvents the Phone with iPhone, 3 pages, 2007, Printed from Website: http://www.apple.com/pr/library/2007/01/09Apple-reinvents-the-phone	
	D1324	Apple Press Info; Apple Announces the New iPhone 3Gs-The Fastest, Most Powerful iPhone Yet, 3 pages, 2009, Printed from the Website: http://www.apple.com/pr/library/2009/06/08Apple-Announces-the-new-iphone3GS	
	D1325	Apple Press Info; Apple Launches iPhone 4S, ios 5 & iCloud, iPhone 4S Features Dual-Core A5 Chip, All New Camera, full 1080p HD Video Recording & Introduces Siri, 2011, 2 pages, Printed from website: http://www.apple.com/pr/library/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud.html	
	D1326	Apple Press Info; Apple Introduces New iPod Touch, Features Retina Display, A4 Chip, FaceTime Video Calling, HD Video Recording & Game Center, 2 pages, 2010, Printed from Website http://www.apple.com/pr/library/2010/09/01Apple-Introduces-New-iPod-touch.html	
	D1327	Apple Press Info; Apple Launches iPad, Magical & Revolutionary Device at an Unbelievable Price, 2 pages, 2010, Printed from Website: http://www.apple.com/pr/library/2010/01/27Apple-Launches-iPad.html	
	D1328	Apple Press Info; Apple Launces New iPad, New iPad Features Retina Display, A5X Chip, 5 Megapixel iSight Camera & Ultrafast 4G LTE, 2012, 3 pages, Printed from the Website: http://www.apple.com/pr/library/2012/03/07Apple-Launches-New-iPad.html	
	D1329	FaceTime; "Phone Calls Like You've Never Seen Before," 3 pages (no date provided)	
	D1330	Apple Press Info; Apple Brings FaceTime to the Mac, 1 pages, Printed from Website https://www.apple.com/pr/library/2010/10/20Apple-Brings-FaceTime-to-the-Mac.html	
	D1331	iPad at Work; "Mobile Meetings Made Easy," 4 pages, 2011	
	D1332	IPad – Technical Specifications, 49 pages, Printed from Website: http://support.apple.com/kb/sp58C	
	D1333	Stirling Design, 8 pages, 2008	
	D1334	Quick Guide: SSL VPN Technical Primer, 11 pages, 2010	
	D1335	Silva, "Secure iPhone Access to Corporate Web Applications," Technical Brief, 10 pages	
	D1336	Defendant Apple Inc.'s Third Supplemental Responses to VirnetX Inc.'s First Request for Admission to Apple Inc. dated, April 13, 2012, 207 pages	
	D1337	Apple Support Communities, 4 pages, Printed from Website https://discussions.apple.com/thread/486096?start=0&tstart=0 (no date)	
	D1338	VirnetX – Products; License and Service Offerings, 1 page (no date provided)	
	D1339	VirnetX Contact Information, 4 pages, 2011	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1340	VirnetX Launches Secure Domain Name Initiative; 4G/LTE Security, 1 page, 2010	
	D1341	VirnetX Gabriel Connection; Enabling Safe Network Neighborhoods, 2 pages, 2012	
	D1342	Baugher et al., "The Secure Real-Time Transport Protocol (SRTP)," Network Working Group, RFC:3711, 39 pages, 2004	
	D1343	Jennings et al., "Resource Location and Discovery (Reload) Draft-Bryan-P2PSIP-Reload-04," Internet-Draft, 12/12/08, pages 1-127	
	D1344	Barnes et al., "Verification Involving PSTN Reachability: Requirements and Architecture Overview," Internet Draft, 27 pages, 2012	
	D1345	April Inc. Form 10-K (Annual Report) filed 12/01/05 for the Period Ending 09/24/05, Edgar Online, 1400 pages, 2011	
	D1346	Phone, Facetime; "Be in Two Places at Once," 3 pages, Printed from the Website http://www.apple.com/ios/facetime/ (no date)	
	D1347	Apple Press Info; Apple Presents iPhone 4, All-New Design with FaceTime Video Calling, Retina, Display, 5 Megapixel Camera & HD Video Recording, 3 pages, 2010	
	D1348	NYSE AMEX:VHC; Cowen and Co. 39th Annual Technology Media & Telecom Conference, 36 pages, June 2, 2011	
	D1349	Pindyck et al., "Market Power: Monopoly and Monopsony," Microeconomics, Sixth Edition, pages 370-371 (no date)	
	D1350	Press Release; IpCapital Group Completes VirnetX IP Licensing Evaluation, 3 pages (no date)	
	D1351	Microsoft Real-Time Communications: Protocols and Technologies, Microsoft TechNet, 22 pages, 2010	
	D1352	Filing Receipt dated September 23, 2011 for Application Number: 13/223,259	
	D1353	Email Communications Regarding Apple Product Innovations, 6 pages, 2010	
	D1354	Mathy et al., "Traversal Using Relays Around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," Internet Engineering Task Force (IETF), RFC: 5766, 67 pages, 2010	
	D1355	Egevang et al., "The IP Network Address Translator (NAT)," Network Working Group, RFC: 1631, 10 pages, 1994	
	D1356	Srisuresh et al., "IP Network Address Translator (NAT) Terminology and Considerations," Network Working Group, RFC:2663, 30 pages, 1999	
	D1357	Sisalem, et al., "Introduction to Cryptographic Mechanisms," SIP Security, 356 pages, 2009	
	D1358	Curriculum Vitae, Mark T Jones, 9 pages (no date)	
	D1359	Curriculum Vitae, Roy Weinstein, 5 pages (no date)	
	D1360	How To Configure IPSec Tunneling in Windows 2000, 8 pages	
	D1361	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/vimetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1362	iPhone, FaceTime; "Be in Two Places at Once," 3 pages, Printed from Website: http://www.apple.com/ios/facetime/ (No date)	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1363	iPhone, "It Does Everything Better,"6 pages, Printed from Website: http://www.apple.com/iPhone/built-in-apps (No date provided)	
	D1364	My Apple ID, "What's an Apple ID," 1 pages, Printed from Website: https://appleid.apple.com/cgi-bin/webobjects/myappleid.woa (no date)	
	D1365	Rosenberg et al., "Session Initiation Protocol (SIP): Locating SIP Servers," Network Working Group, RFC: 3263, 17 pages, 2002	
	D1366	Certified Copy dated September 21, 2012 of Reexamination Certificate Number 6,502,135 issued June 6, 2011, 11 pages	
	D1367	Certified Copy dated September 20, 2012 of Patent Application Number 95/001,269	
	D1368	Chatterjee et al., "Bargaining Under Incomplete Information," Operations Research, 31:835-851, 1983	
	D1369	Nash, "The Bargaining Problem," Econometrica, 18:155-162, 1950	
	D1370	Nash, "Two-Person Cooperative Games," Econometrica, 21:128-140, 1953	
	D1371	Choi et al., "An Analytical Solution to Reasonable Royalty Rate Calculations," IDEA: The Journal of Law and Technology, 13 pages, 2001	
	D1372	The Prize in Economics 1994 - Press Release dated October 11, 1994, 4 pages, Printed from Website: http://www.nobelprize.org/nobel_prizes/economics/laureates/1994/press.html	
	D1373	Putnam et al., "Bargaining and the Construction of Economically Consistent Hypothetical License Negotiations," The Licensing Journal, pages 8-15, 2004	
	D1374	Scherling et al., "Rational Reasonable Royalty Damages: A Return to the Roots," Landslide, Volume 4, 4 pages, 2011	
	D1375	Jarosz et al., "Application of Game Theory to Intellectual Property Royalty Negotiations," Chapter 17, pages 241-265 (no date)	
	D1376	Goldscheider, Licensing Best Practices; Strategic, Territorial, and Technology Issues, 2 pages, 2006	
	D1377	iPhone Configuration Utility, 19 pages, 2012	
	D1378	VPN Server Configuration for iOS Devices, 6 pages, 2012	
	D1379	Samuelson et al., Economics, Fourteenth Edition, pages 258-259, 1992	
	D1380	Stigler et al., The Theory of Price, Forth Edition, pages 215-216, 1987	
	D1381	Truett et al., "Joint Profit Maximization, Negotiation, and the Determinacy of Price in Bilateral Monopoly," Journal of Economic Education, pages 260-270 (no date)	
	D1382	Binmore et al., "Noncooperative Models of Bargaining," The Handbook of Game Theory, 1:(7)181-225,1992	
	D1383	Spindler et al., "Endogenous Bargaining Power in Bilateral Monopoly and Bilateral Exchange," Canadian Journal of Economics-Revue Canadienne D Economie, pages 464-474, 1974	
	D1384	Myerson, "Game Theory; Analysis or Conflict," Harvard University Press, pages 375-392 (no date)	
	D1385	Binmore, "The Nash Bargaining Solution in Economic Modelling," The Rand Journal of Economics, 17:176-188, 1996	

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1386	Rubinstein et al., "On the Interpretation of the Nash Bargaining Solution and its Extension to Non-Expected Utility Preferences," Econometrica, 60:1171-1186, 1992	
	D1387	Greenleaf et al., "Guarantees in Auctions: The Auction House as Negotiator and Managerial Decision Maker," Management Science, 39:1130-1145, 1993	
	D1388	Chan, "Trade Negotiations in a Nash Bargaining Model," Journal of International Economics, 25:253-363, 1987	
	D1389	Lemley et al., "Patent Holdup and Royalty Stacking," Texas Law Review, 85:1991-2049	
	D1390	Cauley, "Winning the Patent Damages Case; A Litigator's Guide to Economic Models and Other Damage Strategies," Oxford Press, pages 29-30, 2044	
	D1391	Degnan et al., "A Survey of Licensed Royalties," Les Nouvelles, pages 91, 93, 94, 1997	
	D1392	Kahn, "The Review of Economics and Statistics," pages 157-164, 1993	
	D1393	Microsoft Company Information; Including Stocks and Financial Information, 83 pages (no date)	
	D1394	Apple Press Info: Apple Updates MacBook Pro with Next Generation Processors, Graphics & Thunderbolt I/O Technology, 3 pages, Printed from Website: http://www.apple.com/pr/library/2011/02/24Apple-Updates-MacBook-Pro-with-Next-Generation-Processors-Graphics-Thunderbolt-I-O-Technology.html	
	D1395	Apple Press Info: Apple to Ship Mac OS X Snow Leopard on August 28, 2 pages, Printed from the Website: http://www.apple.com/pr/library/2009/08/24/apple-to-ship-mac-os-x	
	D1396	iPad, Facetime; "Once Again, iPad gets the World Talking," 3 pages, Printed from the Website: http://www.apple.com/ipad/built-in-apps/facetime/html (no date)	
	D1397	Apple iOS: Setting up VPN, 2 pages, Printed from Website: http/support.apple.com/kb/HT1424 (no date)	
	D1398	Apple iPhone User Guide for iOS 5.1 Software, 179 pages, 2012	
	D1399	Apple, Communicating with HTTP Servers, CFNetworking Programming Guide, 6 pages, 2011, Printed from the Website: https://developer.apple.com/library/ios/documentation/networking/conceptual/CFNetwork/CFHT	
	D1400	VirnetX, Gabriel Connection Technology ™ White Paper, 7 pages, 2012	
	D1401	VirnetX, Technology, 4 pages, 2012	
	D1402	Certified Copy dated January 15, 2008 of U.S. Patent Number 6,502,135, 64 pages	
	D1403	Inter Partes Reexamination Certificate dated June 7, 2011 for Patent Number 6,502,135	
	D1404	Proceedings of The Symposium on Network and Distributed System Security, 7 pages, February 22-23, 1996	
	D1405	In-Q-Tel; Corporate Overview, 2 pages, 2004	
	D1406	Davies, Supervisor of Translation: Tadahiro Uezono, Security for Computer Networks, Japan, Nikkei-McGraw-Hill Inc., First Edition, First Copy, p 126-129 (December 5, 1985) – (English Version and Japanese Version Submitted)	
	D1407	Comer, "Translated by Jun Murai and Hiroyuki Kusumoto, "Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture, Third Edition," Japan Kyoritsu Shuppan Co., Ltd., First Edition, First Copy, p 161-193 (August 10, 1997) (English Version and Japanese Version Submitted)	

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

	D1408	Lynch et al., Supervisor of Translation: Jun Murai, "Internet System Handbook," Japan Impress Co. Ltd. First Edition p 152-157 and p 345-351 (August 11, 1996) (English Version and Japanese Version Submitted)	
	D1409	Office Action dated December 27, 2012 from Corresponding Canadian Patent Application Number 2723504	
	D1410	Office Action dated December 5, 2012 from Corresponding Japanese Patent Application Number 2011-081417	
	D1411	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-085052	
	D1412	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-083415	

EXAMINER /Krisna Lim/	DATE CONSIDERED 05/03/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

CERTIFICATION STATEMENT

This Information Disclosure Statement is being filed after the receipt of the final office action dated December 10, 2012.

The references contained in the Information Disclosure Statement were either; cited in a communication from a foreign patent office in a counterpart foreign application, and, to the was known to any individual designated in § 1.56(c) more than three months prior to the filing of the Information Disclosure Statement, or, received from the client no more than three months prior to the filing of this Information Disclosure Statement.

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

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[X] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or; Cited reference A163 from Canadian office action dated December 27, 2012; Cited reference C25 from Japanese office action dated 12/13/12; Cited references C26, D1254 from Japanese office action dated 12/13/12; C27-C28, D1406-1408 from Japanese office action dated 12/05/12.

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement. Cited references A164-A166 cited by examiner in office action dated December 5, 2012 for U.S. patent application number: 13/617,375; D1255-D1405 all received by the client on January 31, 2013.

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

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $930.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

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

/Toby H. Kusmer/

Date: March 1, 2013

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

DM_US 41379925-1.077580.0154

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson, *et al.*	:	
Serial No.: 13/339,257	:	Confirmation No. 1084
Filed: December 28, 2011	:	Group Art Unit: 2453
Customer Number: 23630	:	Examiner: Lim, Krisna

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

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

Dear Commissioner:

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Applicants thank the Examiner for the Notice of Allowance mailed on May 16, 2013. Without withdrawing the allowed claims from issue, Applicants submit these comments for the record.

In the Statement of Reasons for Allowance included with the Notice of Allowance, the Examiner made certain characterizations and assertions about the allowed claims and certain references cited in the record. (*See* Notice of Allowability at 2.) Although Applicants agree with the Examiner's ultimate conclusion that the claims are patentable, Applicants do not necessarily agree with the Examiner's Statement and the characterizations and assertions therein. The Manual of Patent Examining Procedure and the USPTO rules of practice (37 C.F.R.) require:

"If the examiner believes that the record of the prosecution ***as a whole*** does not make clear his or her reasons for allowing a claim or claims, the examiner may set forth such reasoning." 35 C.F.R. § 1.104. "Each statement should include at least (1) the major difference in the claims not found in the prior art of record, and (2) the reasons why that difference is considered to define patentably over the prior art if either of these reasons for allowance is not clear in the record." M.P.E.P. § 1302.14. "Stock paragraphs with meaningless or uninformative statements of the reasons for the allowance should not be used." (*Id.*)

The Examiner's statements do not comply with these requirements. For example, the Examiner's Statement paraphrases portions of the allowed claims, and emphasizes the paraphrased portions as being the reason the claims are deemed patentable, even though the paraphrased portions do not accurately reflect the language of the allowed claims. Accordingly, the paraphrased portions do not provide a meaningful contribution to the record as it is impossible to determine by the paraphrased portions the difference between the allowed claims and the references cited in the record.

Applicants respectfully submit that each of the allowed claims are patentable based on the subject matter defined by the claim language *as a whole*, and not just by the specific and selective paraphrasing provided by the Examiner.

Furthermore, Applicants understand that the Examiner's characterizations were for purposes of referring to references cited in the record, and do not in any way imply that the claims are limited by words not actually present in the claims. Therefore, Applicants decline to subscribe to any statement or characterization in the Notice of Allowance and the accompanying Examiner's Statement of Reasons for Allowance. Should the Examiner disagree with any of the comments provided herein, the Examiner is invited to contact the undersigned to resolve such disagreement.

If there are any fees due in connection with the filing of this paper, please charge the fees to Deposit Account No. 501133.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: June 21, 2013

/Toby H. Kusmer/

Toby H. Kusmer, P.C., Reg. No. 26,418
Customer No. 23630
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile : (617)535-3800
E-mail: tkusmer@mwe.com

Electronic Acknowledgement Receipt

EFS ID:	16125156
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	21-JUN-2013
Filing Date:	28-DEC-2011
Time Stamp:	21:59:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Post Allowance Communication - Incoming	077580-0154_Comments_Statement_Reasons_Allowance.pdf	99961 878c946de53f685dc50d724a9325202db7a91932	no	3

Warnings:

Information:

Total Files Size (in bytes):	99961

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23630 7590 05/16/2013

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

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

	(Depositor's name)
	(Signature)
	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	12/28/2011	Victor Larson	77580-154(VRNK-1CP3CNFT4)	1084

TITLE OF INVENTION: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$0	$0	$1780	08/16/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LIM, KRISNA	2453	709-204000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 McDermott Will & Emery LLP
2 ____
3 ____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: VirnetX, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Zephyr Cove, NV

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies ____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 501133 (enclose an extra copy of this form).

PTOL-85 (Rev. 02/11)

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

- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature /Toby H. Kusmer/ Date June 21, 2013

Typed or printed name Toby H. Kusmer Registration No. 26,418

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

Electronic Patent Application Fee Transmittal

Application Number:	13339257
Filing Date:	28-Dec-2011
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kimila Carraway
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	1780	1780
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**1780**

Electronic Acknowledgement Receipt

EFS ID:	16125172
Application Number:	13339257
International Application Number:	
Confirmation Number:	1084
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-154(VRNK-1CP3CNFT4)
Receipt Date:	21-JUN-2013
Filing Date:	28-DEC-2011
Time Stamp:	22:32:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1780
RAM confirmation Number	18232
Deposit Account	501133
Authorized User	

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

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

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

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	077580-0154_Issue_Fee_Transmittal.pdf	240533 274d50426eb7af6b988481858c8753d571895b36	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30699 0baf41a707e536d9bc9fb35736d86208b6aa306e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	271232	

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/339,257**
	Filing Date	**12-28-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-154(VRNK-1CP3CNFT4)**

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2002/0004898	1/10/02	Droge	
	B3	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
	B4	US2004/0199493	10/2004	Ruiz et al.	
	B5	US2004/0199520	10/2004	Ruiz et al.	
	B6	US2004/0199608	10/2004	Rechterman et al.	
	B7	US2004/0199620	10/2004	Ruiz et al.	
	B8	US2005/0055306	3/10/05	Miller et al.	
	B9	US2005/0108517	05/2005	Dillon et al.	
	B10	US2006/0059337	03/16/2006	Polyhonen et al.	
	B11	US2006/0123134	06/2006	Munger et al.	
	B12	US2007/0208869	09/2007	Adelman et al.	
	B13	US2007/0214284	09/2007	King et al.	
	B14	US2007/0266141	11/2007	Norton, Michael Anthony	
	B15	US2008/0005792	01/2008	*Larson et al.	
	B16	US2008/0144625	06/2008	Wu et al.	
	B17	US2008/0235507	09/2008	Ishikawa et al.	
	B18	US2009/0193498	07/2009	Agarwal et al.	
	B19	US2009/0193513	07/2009	Agarwal et al.	
	B20	US2009/0199258	08/2009	Deng et al.	
	B21	US2009/0199285	08 ~~09~~/2009	Agarwal et al.	

Change(s) applied to document, /N.A./ 7/9/2013

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 – Number 4 –Kind Code5 *(if known)*	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	C1	DE19924575	12/2/99	Provino et al.			
	C2	EP0814589	12/29/1997	AT&T Corp.			
	C3	EP0838930	4/29/1988	Digital Equipment Corporation			
	C4	EP0858189	8/12/98	Maciel et al.			
	C5	EP836306	4/15/1998	HEWLETT PACKARD CO			
	C6	GB2317792	04/01/1998	Secure Computing Corporation			
	C7	GB2334181	08/11/1999	NEC Technologies			
	C8	GB2340702	02/23/2000	Sun Microsystems Inc.			
	C9	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp			
	C10	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp			
	C11	JP10-070531	03/10/1998	Brother Ind Ltd.			
	C12	JP62-214744	9/21/1987	Hitachi Ltd.			
	C13	WO0070458	11/23/2000	Comsec Corporation			
	C14	WO0017775	3/30/00	Miller et al.			
	C15	WO01016766	03/08/2001	Science Applications International Corporation			
	C16	WO0150688	7/12/01	Kriens			
	C17	WO9827783	06/25/1998	Northern Telecom Limited			
	C18	WO9855930	12/10/98	Tang			

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

/Krisna Lim/ 07/10/2013

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OIPE IAP3 MAR 09 2012 PATENT & TRADEMARK OFFICE

Complete if Known	13339257 - GAU: 2453
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-154(VRNK-1CP3CNFT4)

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Patent Number	Patent Date	Inventor	
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	2,895,502	07/21/1959	Roper et al.	
	A3	4,761,334	08/1988	Sagoi et al.	
	A4	4,885,778	12/5/1989	Weiss, Kenneth	
	A5	4,920,484	4/24/1990	Ranade	
	A6	4,933,846	06/12/1990	Humphrey et al.	
	A7	4,952,930	08/28/1990	Franaszek et al.	
	A8	4,988,990	01/29/1991	Warrior	
	A9	5,164,988	11/17/1992	Matyas	
	A10	5,204,961	04/20/1993	Barlow	
	A11	5,276,735	01/04/1994	Boebert et al	
	A12	5,303,302	04/12/1994	Burrows	
	A13	5,311,593	05/10/1994	Carmi	
	A14	5,329,521	07/12/1994	Walsh et al.	
	A15	5,341,426	08/23/1994	Barney et al.	
	A16	5,367,643	11/22/1994	Chang et al	
	A17	5,384,848	01/24/1995	Kikuchi	
	A18	5,511,122	04/23/1996	Atkinson	
	A19	5,548,646	08/20/1996	Aziz et al.	
	A20	5,559,883	09/24/1996	Williams	
	A21	5,561,669	10/01/1996	Lenney et al	
	A22	5,588,060	12/24/1996	Aziz	
	A23	5,590,285	12/31/1996	Krause et al.	
	A24	5,625,626	04/29/1997	Umekita	
	A25	5,629,984	05/13/1997	McManis	
	A26	5,654,695	08/05/1997	Olnowich et al	
	A27	5,682,480	10/28/1997	Nakagawa	
	A28	5,689,566	11/18/1997	Nguyen	
	A29	5,689,641	11/18/1997	Ludwig et al.	
	A30	5,740,375	04/14/1998	Dunne et al.	
	A31	5,757,925	05/1998	Faybishenko	
	A32	5,764,906	06/1998	Edelstein et al.	
	A33	5,771,239	06/23/1998	Moroney et al.	
	A34	5,774,660	6/30/1998	Brendel et al	
	A35	5,787,172	07/28/1998	Arnold	
Change(s) applied	A36	5,790,548	08/04/1998	~~Sitaraman et al.~~ Sistanizadeh et al.	
to document,	A37	5,796,942	08/18/1998	Esbensen	
/N.A./	A38	5,805,801	09/08/1998	Holloway et al.	
7/9/2013	A39	5,805,803	09/08/1998	Birrell et al.	
	A40	5,822,434	10/13/1998	Caronni et al.	
	A41	5,842,040	11/24/1998	Hughes et al.	
	A42	5,845,091	12/01/1998	Dunne et al.	
	A43	5,864,666	01/1999	Shrader, Theodore Jack London	
	A44	5,867,650	02/02/1998	Osterman	
	A45	5,870,610	02/09/1999	Beyda et al.	
	A46	5,878,231	03 ~~05~~/02/1999	Baehr et al	
	A47	5,892,903	04/06/1999	Klaus	
	A48	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A49	5,905,859	05/18/1999	Holloway et al.	
	A50	5,918,018	06/29/1999	Gooderum et al.	

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

/Krisna Lim/ 07/10/2013

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/339,257	08/06/2013	8504697	77580-154(VRNK-1CP3CNFT4)	1084

23630 7590 07/17/2013

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

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

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

IR103 (Rev. 10/09)