Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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).	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D617	Exhibit Y6: Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC1035").	
	D618	Exhibit Y8: Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997.	
	D619	Exhibit Y8: Woodbum, 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/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D640	Exhibit D-4; Yinger; U.S. Patent 5,960,204 to Yinger et al., "System and Method for Installing Applications on a Computer on an as needed basis, Filed on October 28, 1996 and Issued September 28, 1999	
	D641	Exhibit D-8; Barlow; U.S. Patent 5,204,961 to Barlow, "Computer Network Operating with Multilevel Hierarchical Security with Selectable Common Trust Realms and Corresponding Security Protocols," Filed on June 25, 1990 and Issued April 20, 1993	
	D642	Exhibit D-12; RFC 1122, Braden, "Requirements for Internet Hosts – Communication Layers," RFC 1122 (Oct. 1989)	
	D643	Exhibit D-13; RFC 791; Information Sciences Institute, "Intemet 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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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 *VimetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	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"	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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/ 07/20/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/

07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

07/20/2012

/Krisna Lim/

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

3/26/12 3-26-12 IFW

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

~~13336790 - GAU~~: 2453

OPAP MAR 2 3 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

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

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

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

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

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

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

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

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

SIGNATURE

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

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790

01 FC:1806 180.00 DA

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

DM_US 32511456-1.077580.0151

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

Privacy Act Statement

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

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

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

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

Privacy Act Statement

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

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

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

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

Doc Code: TRAN.LET

Document Description: Transmittal Letter

13336790 - GAU: 2453

PTO/SB/21 (07-09)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Total Number of Pages in This Submission	52
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES (*Check all that apply*)

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ________
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature	Toby H. Kusmer		
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

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

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): ____________

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below
☐ Charge fee(s) indicated below, **except for the filing fee**
☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17
☐ Credit any overpayments

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

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims ______ - 20 or HP = Extra Claims ______ x Fee ($) ______ = Fee Paid ($) ______

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims ______ - 3 or HP = Extra Claims ______ x Fee ($) ______ = Fee Paid ($) ______

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims: Fee ($) ______ Fee Paid ($) ______

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ______ - 100 = Extra Sheets ______ / 50 = Number of each additional 50 or fraction thereof ______ (round up to a whole number) x Fee ($) ______ = Fee Paid ($) ______

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature	[signature]	Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

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

13336790 - GAU: 2453

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

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

Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

OPAP MAR 2 3 2012 IAP23 PATENT & TRADEMARK OFFICE

☒ Transmittal Letter

X IDS FORM 1449 (50 pages)

X 16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

☒ Fee Transmittal

☐ Response to Missing Parts Notice

☐ Copy of Missing Parts Notice

☐ Replacement Drawing

☐ Maintenance Fee for ______ years after grant

☐ Fee Address Indication Form

☐ Terminal Disclaimer

☐ Petition to Commissioner

☐ Status Inquiry

☒ Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	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	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

CERTIFICATION STATEMENT

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

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

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

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

[X] The Commissioner is hereby authorized to charge 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 37789411-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	13592862
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	27-AUG-2012
Filing Date:	23-DEC-2011
Time Stamp:	13:32:48
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	65568 8c3179d6c9193eea99933f477cbb0092c6da8669	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	D1217.pdf	11161127 15c3902ff98d5442223a0deb429324c4c088740f	no	211
Warnings:					
Information:					
3	Non Patent Literature	D1218.pdf	171392 4de801f2c5f80805bb67088e6b5e9cc7c3df0153	no	4
Warnings:					
Information:					
4	Non Patent Literature	D1215__.pdf	2340352 8cf0f73ee68d707c41f500ca2993ab39cefe7acb	no	282
Warnings:					
Information:					
5	Non Patent Literature	D1216_.pdf	253751 2bedf1012dc0d5ca841e8957fd504aaa3c8d9a2e	no	55
Warnings:					
Information:					
6	Non Patent Literature	D1219_.pdf	300469 88a75e44bb96dc311611481970f8b2ebfb3d2fee	no	69
Warnings:					
Information:					
			Total Files Size (in bytes):	14292659	

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:	13594950
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	27-AUG-2012
Filing Date:	23-DEC-2011
Time Stamp:	15:16:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1215part1_.pdf	6004542 ba8668057be3412bd85bc98b35f3ffbc3063d76a	no	1446

Warnings:

Information:

2	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:

Total Files Size (in bytes):	9010047

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.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 09/04/2012
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
09/04/2012	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.** 13/336,790	**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: *23 August 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 proposed 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	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	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	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

[X] The Commissioner is hereby authorized to charge 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: 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 38996721-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	13820387
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	24-SEP-2012
Filing Date:	23-DEC-2011
Time Stamp:	15:19:18
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	70656 eecb302b975c9150b3bfb5ff7b446791eb477ea2	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 9ce2ace217ce1e1fbae718ae13ac16c5629341a3	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 2ebd0940ee6e4b3f4a822663b789030d32c09246	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 babcedd540231da1cc3e3494f36e2cbdfb1ff7d7	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 00410f7202c99c99c2f118d5fbe6a3adb83461be	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):			1045850		

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

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

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

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	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 Swith 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	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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 Demonstations 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 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

[ ] 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: 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 39143875-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	13902670
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	04-OCT-2012
Filing Date:	23-DEC-2011
Time Stamp:	12:49:56
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	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	97478 dabcbb8cd87a5cf35a78f3c19adf0a3c77b28b70	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 c0c023e1ffceb4909f65537ac685570ce8900 0f0	no	25
Warnings:					
Information:					
3	Non Patent Literature	D1226.PDF	9200782 8580c9a4640bf44fb6e2957b63f29a731ecfc 9df	no	122
Warnings:					
Information:					
4	Non Patent Literature	D1227.PDF	1923180 c3f5782b90fe6dd48d635c349d737d268f6c ff2e	no	2
Warnings:					
Information:					
5	Non Patent Literature	D1228.PDF	4527086 38650c0ad25030424906589531 82f34c882 385d5	no	7
Warnings:					
Information:					
6	Non Patent Literature	D1229.PDF	1921619 8a30921b2a6d77e3745af10f4b4208a362fb dd58	no	2
Warnings:					
Information:					
7	Non Patent Literature	D1230.PDF	7300485 bc94176849e0031bdfa94581437d293ad31 e622a	no	6
Warnings:					
Information:					
8	Non Patent Literature	D1231.PDF	6455029 1dae9c7575280f98a1b9665ebecf8047f644 e308	no	94
Warnings:					
Information:					
9	Non Patent Literature	D1232.PDF	936879 a64c3cc70a981e525fa1c2a0856466016fec 4742	no	21
Warnings:					
Information:					

10	Non Patent Literature	D1233.PDF	2643873 0ad9db0a2c4d60a911bbea292e56064556 9beb42	no	34
Warnings:					
Information:					
11	Non Patent Literature	D1234.PDF	1337280 26f30a98ca4b3c06dee097790ecccd22ed1c d625	no	17
Warnings:					
Information:					
12	Non Patent Literature	D1235.PDF	1118077 570378cf0fef9a9f0db5934767a10631a969 7ccb	no	17
Warnings:					
Information:					
13	Non Patent Literature	D1236.PDF	516087 43622ea13fa2edcf841bf78b01ea08c61ecc ef68	no	7
Warnings:					
Information:					
14	Non Patent Literature	D1237.PDF	978889 cb31cc3954935b83adf852ae9cd68114d72 e63d9	no	15
Warnings:					
Information:					
15	Non Patent Literature	D1238.PDF	2081715 7b840029a950da75a9c9adb76c6f30c69e1 88862	no	24
Warnings:					
Information:					
16	Non Patent Literature	D1239.PDF	329750 2d833f9187957eedcb0e407a1356ea87c36 e052e	no	5
Warnings:					
Information:					
17	Non Patent Literature	D1240.PDF	507540 a74f5d5fbe671acf2414f22eaec9bbb487ffb 0e2	no	8
Warnings:					
Information:					
18	Non Patent Literature	D1241.PDF	6401651 62ec4bfa8bce771c05b216d7c47c403a529 73f36	no	116
Warnings:					
Information:					

19	Non Patent Literature	D1242.PDF	5607358 8f2f53edf2efb6f020153bbe73c2b562a03bb4f7	no	102
Warnings:					
Information:					
20	Non Patent Literature	D1243.PDF	7301095 3e89def78808ab4f8f5ce0b234cd3322f595cd61	no	130
Warnings:					
Information:					
			Total Files Size (in bytes):	62570862	

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:	13904908
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	04-OCT-2012
Filing Date:	23-DEC-2011
Time Stamp:	15:25:38
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	D1244.PDF	7945433 417911827dcb8d869eb9e217f1414dc9c4a46f9d	no	138

Warnings:

Information:

2	Non Patent Literature	D1245.PDF	17791506 735e0d644c3a58450a4b6cf096d32db096ca6d70	no	304
Warnings:					
Information:					
3	Non Patent Literature	D1246.PDF	17791522 be912d02c9cba1b615568dab376ef177ef963f86	no	304
Warnings:					
Information:					
4	Non Patent Literature	D1250.PDF	4663415 eedc19be973a322d4836e6d220271020c082e15f	no	92
Warnings:					
Information:					
5	Non Patent Literature	D1251.PDF	5973935 fac713d79db8ae257186853a6ddb06f093b63bec	no	113
Warnings:					
Information:					
6	Non Patent Literature	D1252.PDF	6581540 2caebc0aacfb81210ecf5bbcf02440006b76a065	no	118
Warnings:					
Information:					
7	Non Patent Literature	D1253.PDF	1740859 7ea0a705b2f08195bb7ab0b072b732bef178620e	no	4
Warnings:					
Information:					
8	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:					
9	Non Patent Literature	D1247part2.pdf	4380602 f9d82845d47589474fcfc6f26b8fe686384ccef5	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:					

10	Non Patent Literature	D1248part1.pdf	5121910 110aa00905f6405ddd299e00b45cf87c67621cd0	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:					
11	Non Patent Literature	D1248part2.pdf	4580517 8369e89c947d049595d9e6451f6f84006b949fc4	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:					
12	Non Patent Literature	D1249part1.pdf	4350698 6ce20ea7a52e3038ca51c565713640627d230135	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:					
13	Non Patent Literature	D1249part2.pdf	4232123 2bdcf1c426a5631c6be840dc2307b3a0751b50b2	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:					
14	Non Patent Literature	D1249part3.pdf	3557941 200eca2c1f3735e7560f74449c981de155573a10	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:					
			Total Files Size (in bytes):	93190738	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	D1225	VPN 3000 Concentrator Series, User Guide; Release 2.5 July 2000 (489 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 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

[ ] 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: October 5, 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 39180174-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	13915884
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	05-OCT-2012
Filing Date:	23-DEC-2011
Time Stamp:	10:04:45
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	55823 b45f43898dbdb8b231b5b501360a15b1c5987943	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	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:					
3	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:					
Total Files Size (in bytes):			17816741		

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 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.** 13/336,790	**Applicant(s)** LARSON ET AL.	
	Examiner KRISNA LIM	**Art Unit** 2453	

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

(1) *KRISNA LIM*. (3) *Mr. Robert Short*.

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

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.: 13/336,790	:	Confirmation No. 6217
Filed: December 23, 2011	:	Group Art Unit: 2453
Customer Number: 23630		Examiner: Lim, Krisna

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

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

REPLY "B"

Dear Commissioner:

This Reply is being filed in response to the Office Action mailed from the United States Patent and Trademark Office on July 27, 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 7 of this paper.

IN THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in this application.

LISTING OF CLAIMS:

1. (Presently Amended) A network device, comprising:

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

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

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

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

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

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

2. (Original) The network device of claim 1, wherein:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

29. (New) The network device of claim 1, wherein the interception of the request consists of receiving the request to determine that the second network device is available for the secure communication service.

30. (New) The method of claim 15, wherein the interception of the request consists of receiving the request to determine that the second network device is available for the secure communication service.

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

32. (New) The method of claim 15, wherein the interception occurs within another network device that is separate from the first network device.

REMARKS

Claims 1-13, 15-27, and 29-32 are pending in the application, of which claims 1 and 15 are the only independent claims. By this Amendment, Applicants amend independent claims 1 and 15, add new dependent claims 29-32, and cancel claims 14 and 28 without prejudice or disclaimer of the subject matter thereof.[1] In the Office Action mailed July 27, 2012 ("Office Action"), claims 1-13 and 15-27 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.

Applicants' Summary and Clarification of the August 23, 2012 and October 11, 2012 Interviews

Applicants appreciate the courtesies extended to Applicants' undersigned representative at the personal interview conducted in the United States Patent and Trademark Office on August 23, 2012 ("first interview"), as well as to Applicants' undersigned representative and inventor Dr. Robert Short III at the personal interview on October 11, 2012 ("second interview"). The Examiner mailed Interview Summaries on September 4, 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.

In the first interview, Applicants' undersigned 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 of the claimed subject matter over firewall systems such as *Wesinger*'s. The Examiner suggested that an exemplary feature discussed by Applicants'

[1] Applicants disagree that the original claims submitted on December 23, 2011 are disclosed or obvious over the prior art. However, Applicants amend the claims to expedite prosecution of this matter as explained in this response. 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.

representative and Dr. Short while providing the overview — 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 — was distinguishable over the prior art. As such, the Examiner suggested that Applicants amend the claims accordingly.

However, in the second Interview Summary, the Examiner summarized the discussions of such allowable features as the "gist of the invention." Although Applicants agree that "receiving, following interception of the request and a determination that the second network device is available for the secure communication service, an indication that the second network device is available for the secure communications service, the requested network address of the second network device, and provisioning information for a virtual private network communication link" is one feature that distinguishes the disclosed subject matter 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 Amendment. Thus, while Applicants have amended certain claims based on the Examiner's suggestion to expedite allowance of this application, Applicants submit that the unamended claims are patentably distinguished from *Wesinger* and other cited prior art.

Claim Rejections – 35 U.S.C. § 103

Claims 1-13 and 15-27 are rejected under 35 U.S.C. § 103(a) over *Wesinger*. As explained below, because *Wesinger* does not disclose or suggest each and every limitation of claims 1-13 and 15-27, Applicants request that the rejection be withdrawn and the claims be allowed.

To support an obviousness 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)) (emphases 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 1-13 and 15-27 are disclosed or suggested by *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 transparent 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 than the embodiments recited in claims 1-13 and 15-32. For instance, independent claim 1 is representative and recites:

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

Wesinger does not disclose receiving "an indication that the second network device is available for the secure communications service, the requested network address of the second network device, and provisioning information for a virtual private network communication link," as recited in claim 1. Nor does *Wesinger* disclose the ability to "connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link" and "communicate with the second network device using the secure communications service via the virtual private network communication link," as recited in claim 1. For these reasons alone, the rejection of claim 1 in view of *Wesinger* is improper and should be withdrawn.

For example, nothing in *Wesinger*, including at the cited portions, teaches or suggests at least the feature of enabling a network device to "receive . . . an indication that the second network device is available for the secure communications service," as recited by claim 1. The virtual hosts and DNS mappings of *Wesinger* enable transparent communications through the firewall, but provide no such indication that the second network device is available for a secure communications service.

Wesinger briefly states that encryption may be used in combination with its firewalls, but does not describe those firewalls as providing any indication that a second device is available for the secure communications service. (*See Wesinger* at 4:39-42; 12:22-28.) In fact, *Wesinger* explains 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 enabling a network device to receive an indication that the second network device is available for the secure communications service. *Wesinger* invokes the code that performs channel processing and encryption without returning any indication that the second device is available for a secure communications service.

The Office Action points to a portion of *Wesinger* that describes a piece of software checking whether the host "requesting the connection"[2] has a DNS entry in a database. (OA at 3 (citing *Wesinger* at 16:57-17:5).) However, following that check, *Wesinger* does not enable the device requesting the connection to receive an indication that the second network device is available for a secure communications service. Thus, that passage of *Wesinger*, does not demonstrate the claimed features. (*See Wesinger* at 16:57-67.)

Moreover, *Wesinger* merely describes returning a network address of a virtual host. (*Id.* at 9:15-25.) *Wesinger* makes it clear that the network address is returned alone, and not with

[2] *Wesinger* defines a "remote host" as the "host requesting the connection" for the purpose of the cited paragraphs. (*Wesinger* at 16:49.)

"provisioning information." Consequently, *Wesinger*, does not teach or suggest "receiving . . . provisioning information for a virtual private network" (emphasis added), as recited by claim 1. Indeed, in *Wesinger*, after a connection request is received and allowed, the virtual host invokes code that performs channel processing (including encryption) but does not return any provisioning information for a virtual provide network. (*Id.* at 17:1-7.) Aside from the address, nothing else is returned to the requesting device in *Wesinger*.

For the above reasons alone, *Wesinger* does not support the rejection of claim 1 under 35 U.S.C. § 103(a). Accordingly, the rejection should be withdrawn, and the claim should be allowed.

In addition to the distinguishing features set forth above, claim 1 is further allowable over *Wesinger* because the reference does not disclose the ability to receive the claimed indication "following interception of the request and a determination that the second network device is available for the secure communication service," as recited in amended claim 1. This feature is consistent with the subject matter that the Examiner identified as distinguishing over the prior art during the second interview. Indeed, the Examiner agreed during the second interview that *Wesinger* fails to disclose or suggest intercepting a request to look up a network address of a network device and determining that the network device is available for a secure communications service at all. For this additional reason, *Wesinger* does not disclose or suggest all of the features of independent claim 1. As a result, the rejection of claim 1 in view of *Wesinger* is improper, should be withdrawn, and claim 1 should be allowed.

Accordingly, since *Wesinger* does not teach or suggest at least the claimed features of enabling a network device to "receive an indication that the second network device is available for the secure communications service" or "provisioning information for a virtual private network" at all, much less "following interception of the request [to look up the network address of the second network device] and a determination that the second network device is available for a secure communications service," 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 reasons similar to those provided above for independent claim 1, *Wesinger* does not teach or suggest each and every limitation of independent claim 15. Consequently, for the same reasons set forth above for claim 1, *Wesinger* does not support the rejection of claim 15 under 35 U.S.C. § 103(a). Thus, the rejection should be withdrawn and the claim should be allowed.

Claims 2-13, 29, and 31 depend from claim 1. Claims 16-27, 30, and 32 depend from claim 15. Thus, for at least the same reasons set forth above in connection with claims 1 and 15, dependent claims 2-13, 16-27, and 29-32 are allowable over the cited prior art. Additionally, dependent claims 2-13, 16-27, and 29-32 are allowable for the additional reason that each of the claims recite additional features not disclosed or suggested by the cited prior art. Accordingly, Applicants request the timely allowance of these claims.

CONCLUSION

Applicants respectfully submit that all of the pending claims, claims 1-13, 15-27, and 29-32, are allowable over the cited prior art. 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 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. Indeed, as noted above, Applicants disagree that the original claims submitted on December 23, 2011 are disclosed or suggested by the cited prior art, and reserve the right to pursue protection of embodiments covered by that scope, and other aspects of Applicants disclosed embodiments, in one or more continuation applications.

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 26, 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

DM_US 39458774-1.077580.0151

Electronic Patent Application Fee Transmittal

Application Number:	13336790
Filing Date:	23-Dec-2011
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Tricia Tedesco
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
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:	14088068
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Tricia Tedesco
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	26-OCT-2012
Filing Date:	23-DEC-2011
Time Stamp:	16:33:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$124
RAM confirmation Number	3595
Deposit Account	501133
Authorized User	

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

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

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

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ReplyB.pdf	130493 a886feda3c1fb3e3157cf4d169b6552ef865cecd	no	14
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30626 12643cc8076bd98fd14748087af611c5a46014e9	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	161119	

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.

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	Filing Date	To be Mailed
13/336,790	12/23/2011	☐

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

10/26/2012	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))	* 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

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)	OR	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:
/GAIL WOOTEN/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson *et al.*	:	
Serial No.: 13/336,790	:	Confirmation No. 6217
Filed: December 23, 2011	:	Group Art Unit: 2453
Customer Number: 23630	:	Examiner: Lim, Krisna

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

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

SUPPLEMENTAL REPLY "C"

Dear Commissioner:

This Supplemental Reply is being filed further to Applicants' October 26, 2012, response to the Office Action mailed from the United States Patent and Trademark Office on July 27, 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 7 of this paper.

IN THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in this application.

LISTING OF CLAIMS:

1. (Presently Amended) A network device, comprising:

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

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

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

receive, following interception of the request and a determination that the second network device is available for the secure communication service, an indication that the second network device is available for the secure communications service, the requested IP ~~network~~ address of the second network device, and provisioning information for a virtual private network communication link;

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

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

2. (Original) The network device of claim 1, wherein:

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

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

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

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

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

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

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

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

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

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

11. (Canceled)

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

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

14. (Canceled)

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

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

following interception of the request and a determination that the second network device is available for the secure communication service, receiving an indication that the second network device is available for a secure communications service, the requested ~~network~~ IP address of the second network device, and provisioning information for a virtual private network communication link; [[and]]

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

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

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

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

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

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

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

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

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

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

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

25. (Canceled)

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

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

28. (Canceled)

29. (Previously presented) The network device of claim 1, wherein the interception of the request consists of receiving the request to determine that the second network device is available for the secure communication service.

30. (Previously presented) The method of claim 15, wherein the interception of the request consists of receiving the request to determine that the second network device is available for the secure communication service.

31. (Previously presented) The network device of claim 1, wherein the interception occurs within another network device that is separate from the network device.

32. (Previously presented) The method of claim 15, wherein the interception occurs within another network device that is separate from the first network device.

REMARKS

Claims 1-10, 12, 13, 15-24, 26, 27, and 29-32 are pending in the application, of which claims 1 and 15 are the only independent claims. By this Amendment, Applicants amend independent claims 1 and 15, and cancel claims 11 and 25 without prejudice or disclaimer of the subject matter thereof.[1] The Office Action mailed July 27, 2012 ("Office Action") rejects claims 1-10, 12, 13, 15-24, 26, and 27 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.

Summary of Telephone Interview

Applicants appreciate the courtesies extended to Applicants' representatives during the November 15, 2012, telephone interview. During the interview, the Examiner and Applicants' representatives discussed potential claim amendments. The Examiner agreed that the independent claims as they are currently amended by this supplemental amendment are not disclosed or suggested by the prior art of record, and that he would withdraw the rejection and allow the pending claims if Applicants amended the claims as proposed in this supplemental amendment.

Claim Rejections – 35 U.S.C. § 103

The July 27, 2012, Office Action rejects claims 1-10, 12, 13, 15-24, 26, and 27 under 35 U.S.C. § 103(a) over *Wesinger*. For at least the reasons discussed in the October 26, 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 November 15, 2012, 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 they are currently amended by this supplemental amendment. Thus, while Applicants maintain that both the

---

[1] Applicants disagree that the original claims submitted on December 23, 2011 or the amended claims submitted in the amendment filed on October 26, 2012 are disclosed or obvious over the prior art. However, Applicants amend the claims to expedite prosecution of this matter as explained in this response. Applicants reserve the right to pursue patent protection for the embodiments recited in the original and/or previously amended claims and variants thereof, in one or more continuation applications.

original claims presented on December 23, 2011, and the claims presented in response of October 26, 2012 distinguish over *Wesinger*, and any other prior art of record, Applicants amend the claims as listed above solely to expedite prosecution of this application.

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 withdrawal of the § 103 rejection of the claims and the timely allowance of all pending claims 1-10, 12, 13, 15-24, 26, 27, and 29-32.

CONCLUSION

Applicants respectfully submit that all pending claims 1-10, 12, 13, 15-24, 26, 27, and 29-32 are allowable over the cited references. 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 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. Indeed, as noted above, Applicants disagree that the original claims submitted on December 23, 2011 are disclosed or suggested by the cited prior art, and reserve the right to pursue protection of embodiments covered by that scope, and other aspects of Applicants disclosed embodiments, in one or more continuation applications.

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: November 15, 2012

/Toby H. Kusmer/

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

DM_US 39843905-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	14240529
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Tricia Tedesco
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-NOV-2012
Filing Date:	23-DEC-2011
Time Stamp:	17:03:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SupplementalReplyC.pdf	111655 ca5dbc90abae195a2be67749932be20e61b64c25	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Supplemental Response or Supplemental Amendment	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	9

Warnings:

Information:

Total Files Size (in bytes):	111655

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	Filing Date	
13/336,790	12/23/2011	☐ 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 11/15/2012	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 28	Minus	** 30	= 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 PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 11/20/2012

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
11/20/2012	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.** 13/336,790	**Applicant(s)** LARSON ET AL.	
	Examiner KRISNA LIM	**Art Unit** 2453	

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

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

(2) *Mr. Toby Kusmer (Reg. No. 26,418)*. (4)_____.

Date of Interview: *14 November 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 Examienr discussed the amended language of claim 1 (lines 5-6). No agreement was 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	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A163	5,345,439	09/06/1994	Marston	
	A164	5,884,038	03/16/1999	Kapoor	
	A165	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 Code5 *(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.

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**13/336,790**
				Filing Date	**12-23-2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Krisna Lim**
				Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

[ ] The Commissioner is hereby authorized to charge 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: 12/10/12

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 40181450-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	14433789
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	11-DEC-2012
Filing Date:	23-DEC-2011
Time Stamp:	15:32:51
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	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	66687 5e223712d28a3366d9bfa19231526442b3d97acb	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	
Total Files Size (in bytes):	66687

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 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 01/10/2013

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: 01/10/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

TITLE OF INVENTION: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$0	$0	$1770	04/10/2013

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 SMALL ENTITY status shown above.

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

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

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

If the SMALL ENTITY is shown as NO:

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

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

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23630 7590 01/10/2013

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.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

TITLE OF INVENTION: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$0	$0	$1770	04/10/2013

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

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

Authorized Signature ______________________________ Date ______________________________

Typed or printed name ______________________________ Registration No. ______________________________

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 01/10/2013

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: 01/10/2013

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.

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. 13/336,790	Applicant(s) LARSON ET AL.	
	Examiner KRISNA LIM	Art Unit 2453	

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

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 11/15/2012 and 10/26/2012*.
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 *1-10,12,13,15-24,26,27 and 29-32*. 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).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Krisna Lim/
Primary Examiner, Art Unit 2453

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 host) 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 1-10, 12-13, 15,-24, 26-27 and 29-32 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
December 21, 2012

/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	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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

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 12/21/2012

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

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

[ ] 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: 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 38996721-1.077580.0151

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	D1225	VPN 3000 Concentrator Series, User Guide; Release 2.5 July 2000 (489 pages)	

EXAMINER /Krisna Lim/	DATE CONSIDERED 12/21/2012

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

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

[ ] 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: October 5, 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 39180174-1.077580.0151

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	A1121	Declaration of Angelos D. Keromytis, Ph.D.	
	A1122	Declaration of Dr. Robert Dunham Short III	
	A1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.)	
	A1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. (Control No. 95/001,269)	
	A1125	Exhibit A-4, Redacted Deposition of Chris Hopen from VirnetX, Inc. v. Cisco Systems, Inc., No. 6:07-CV 417 (E.D. Tex. April 11, 2012)	
	A1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, (Feb. 1999)	
	A1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects	
	A1128	Exhibit B-3, Maryann Lawlor, Transient Partnerships Stretch Security Policy Management, Signal Magazine (Sept. 2001) http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes	
	A1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html.	
	A1130	Time Greene, CEO's Chew the VPN Fat, CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	07/20/2012

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

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

[ ] None

SIGNATURE

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

Toby H. Kusmer

Date: 5/18/12

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

DM_US 35089818-1.077580.0151

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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]	

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1146	Exhibit 232A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '504 Patent[2]	
	D1147	Exhibit 233A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '759 Patent[2]	
	D1148	Exhibit 255, Schulzrinne[1] vs. Claims of the '135 Patent[2]	
	D1149	Exhibit 256, Schulzrinne[1] vs. Claims of the '504 Patent[2]	
	D1150	Exhibit 257, Schulzrinne[1] vs. Claims of the '211 Patent[2]	
	D1151	Exhibit 258, Schulzrinne[1] vs. Claims of the '151 Patent[2]	
	D1152	Exhibit 259, Schulzrinne[1] vs. Claims of the '180 Patent[2]	
	D1153	Exhibit 260, Schulzrinne[1] vs. Claims of the '759 Patent[2]	
	D1154	Exhibit 261, SSL 3.0[1] vs. Claims of the '151 Patent[2]	
	D1155	Exhibit 262, SSL 3.0[1] vs. Claims of the '759 Patent[2]	
	D1156	Exhibit 263, Wang[1] vs. Claims of the '135 Patent[2]	
	D1157	Wang[1] vs. Claims of the '504 Patent[2]	
	D1158	Wang[1] vs. Claims of the '211 Patent[2]	
	D1159	Exhibit 1, Alexander CV.pdf	
	D1160	Exhibit 2, Materials Considered by Peter Alexander	
	D1161	Exhibit 3, Cross Reference Chart	
	D1162	Exhibit 4, RFC 2543[1] vs. Claims of the '135 Patent	
	D1163	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent	
	D1164	Exhibit 6, RFC 2543[1] vs. Claims of the '211 Patent	
	D1165	Exhibit 7, The Schulzrinne Presentation[1] vs. Claims of the '135 Patent	
	D1166	Exhibit 8, The Schulzrinne Presentation[1] vs. Claims of the '504 Patent	
	D1167	Exhibit 9, The Schulzrinne Presentation[1] vs. Claims of the '211 Patent	
	D1168	Exhibit 10, The Schulzrinne Presentation[1] vs. Claims of the '151 Patent	
	D1169	Exhibit 11, The Schulzrinne Presentation[1] vs. Claims of the '180 Patent	
	D1170	Exhibit 12, The Schulzrinne Presentation[1] vs. Claims of the '759 Patent	
	D1171	Exhibit 13, SSL 3.0[2] vs. Claims of the '135 Patent	
	D1172	Exhibit 14, SSL 3.0[2] vs. Claims of the '504 Patent	
	D1173	Exhibit 15, SSL 3.0[2] vs. Claims of the '211 Patent	
	D1174	Exhibit 16, SSL 3.0[2] vs. Claims of the '151 Patent	
	D1175	Exhibit 17, SSL 3.0[2] vs. Claims of the '759 Patent	
	D1176	Exhibit 18, Kiuchi[1] vs. Claims of the '135 Patent	

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1177	Exhibit 19, Kiuchi[1] vs. Claims of the '504 Patent	
	D1178	Exhibit 20, Kiuchi[1] vs. Claims of the '211 Patent	
	D1179	Exhibit 21, Kiuchi[1] vs. Claims of the '151 Patent	
	D1180	Exhibit 22, Kiuchi[1] vs. Claims of the '180 Patent	
	D1181	Exhibit 23, Kiuchi[1] vs. Claims of the '759 Patent	
	D1182	Exhibit 24, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '135 Patent	
	D1183	Exhibit 25, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '504 Patent	
	D1184	Exhibit 26, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '211 Patent	
	D1185	Exhibit 27, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '151 Patent	
	D1186	Exhibit 28	
	D1187	Exhibit 29, The Altiga System[1] vs. Claims of the '135 Patent	
	D1188	Exhibit 30, The Altiga System[1] vs. Claims of the '504 Patent	
	D1189	Exhibit 31, The Altiga System[1] vs. Claims of the '211 Patent	
	D1190	Exhibit 32, The Altiga System[1] vs. Claims of the '759 Patent	
	D1191	Exhibit 33, U.S. Patent No. 6,496,867 ("Beser")[1] and RFC 2401[2] vs. Claims of the '135 Patent	
	D1192	Exhibit 34, U.S. Patent No. 6,496,867 ("Beser")[1] and RFC 2401[2] vs. Claims of the '504 Patent	
	D1193	Exhibit 35, U.S. Patent No. 6,496,867 ("Beser")[1] and RFC 2401[2] vs. Claims of the '211 Patent	
	D1194	Exhibit 36, U.S. Patent No. 6,496,867 ("Beser")[1] and RFC 2401[2] vs. Claims of the '151 Patent	
	D1195	Exhibit 37, U.S. Patent No. 6,496,867 ("Beser")[1] and RFC 2401[2] vs. Claims of the '180 Patent	
	D1196	Exhibit 38, Kent[1] vs. Claims of the '759 Patent	
	D1197	Exhibit 39, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent[2]	
	D1198	Exhibit 40, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent[2]	
	D1199	Exhibit 41, Aziz ('646)[1] vs. Claims of the '759 Patent	
	D1200	Exhibit 42, The PIX Firewall[1] vs. Claims of the '759 Patent	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	07/20/2012

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

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

[ ] None

SIGNATURE

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

Toby H Kusmer

Date: 6/1/12

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

DM_US 35497951-1.077580.0151

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	D1208	Cisco Comments and Petition for Reexamination 95/001,679 dated June 14, 2012	
	D1209	Exhibit S, Declaration of Nathaniel Polish, Ph.D.	
	D1210	Exhibit R, Excerpts from Patent Owner & Plaintiff VirnetX Inc.'s First Amended P.R. 3-1 and 3-2 Disclosure of Asserted Claims and Infringement Contentions	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

[ ] None

SIGNATURE

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

Date: 6/20/12

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

DM_US 36051951-1.077580.0151

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	D1211	Third Party Requester Comments dated June 25, 2012 - After Non Final Office Action (95/001,788)	
	D1212	Reexam Affidavit/Declaration/Exhibit Filed by 3rd Party on June 25, 2012 (95/001,788)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	07/20/2012

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

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

[ ] None

SIGNATURE

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

Toby H. Kusmer

Date: 6/28/12

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

DM_US 36237561-1.077580.0151

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	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 12/21/2012

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

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

SIGNATURE

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

Date: 7/24/12

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

DM_US 36887772-1.077580.0151

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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/	12/21/2012

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

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

[ ] 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 37789411-1.077580.0151

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	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 Swith 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	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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 Demonstations and Testing, are also Described in Marketing Materials and Publications (4 pages)	

EXAMINER /Krisna Lim/	DATE CONSIDERED 12/21/2012

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

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

[X] The Commissioner is hereby authorized to charge 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: 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 39143875-1.077580.0151

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A163	5,345,439	09/06/1994	Marston	
	A164	5,884,038	03/16/1999	Kapoor	
	A165	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 Code5 *(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 12/21/2012

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

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

[ ] The Commissioner is hereby authorized to charge 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: 12/10/12

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 40181450-1.077580.0151

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A161	6,131,121	10/10/2000	Mattaway et al.	
	A162	6,499,108	12/24/2002	Johnson	

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Code5 (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

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

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1112	ITU-T Recommendation H.323, "Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System," International Telecommunications Union, pages 1-128, February 1998	
	A1113	ITU-T Recommendation H.225.0, "Infrastructure of Audiovisual Services – Transmission Multiplexing and Synchronization. Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication systems," International Telecommunication Union, pages 1-155, February 1998	
	A1114	ITU-T Recommendation H.235, "Infrastructure of Audiovisual Services – Systems Aspects. Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals," International Telecommunication Union, pages 1-39, February 1998	
	A1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	A1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	A1117	Transmittal Letters (Patent No.8,051,181)	
	A1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	07/20/2012

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

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

[ ] None

SIGNATURE

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

Date: 4/24/12

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

DM_US 33806475-1.077580.0151

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

Index of Claims	Application/Control No. 13336790	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	07/20/2012	12/21/2012						
1	1	✓	✓	=						
2	2	✓	✓	=						
3	3	✓	✓	=						
4	4	✓	✓	=						
5	5	✓	✓	=						
6	6	✓	✓	=						
7	7	✓	✓	=						
8	8	✓	✓	=						
9	9	✓	✓	=						
10	10	✓	✓	=						
	11	✓	✓	-						
12	12	✓	✓	=						
13	13	✓	✓	=						
	14	✓	✓	-						
15	15	✓	✓	=						
16	16	✓	✓	=						
17	17	✓	✓	=						
18	18	✓	✓	=						
19	19	✓	✓	=						
20	20	✓	✓	=						
21	21	✓	✓	=						
22	22	✓	✓	=						
23	23	✓	✓	=						
24	24	✓	✓	=						
	25	✓	✓	-						
26	26	✓	✓	=						
27	27	✓	✓	=						
	28	✓	✓	-						
11	29			=						
25	30			=						
14	31			=						
28	32			=						

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13336790	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

ORIGINAL		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)				

☐ 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	24												
9	9		25												
10	10	26	26												
	11	27	27												
12	12		28												
13	13	11	29												
	14	14	30												
15	15	25	31												
16	16	28	32												

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 28	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 (Primary Examiner)	12/21/2012 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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/	07/20/2012

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

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2165**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

[ ] None

SIGNATURE

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

Toby H. Kusmer

Date: 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 34023885-1.077580.0151

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

Search Notes	Application/Control No. 13336790	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 2453

SEARCHED

Class	Subclass	Date	Examiner
709	223-227	02/23/2012	kl
	updated above	07/20/2012	kl
709	223-227	12/21/2012	kl

SEARCH NOTES

Search Notes	Date	Examiner
East, Inventors	02/23/2012	kl
Inventors, all the prior arts submitted by applicants	12/21/2012	kl

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
709	223-227	12/21/2012	kl

3-26-12

TFW

13336790 - GAU 2453

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP MAR 2 3 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

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

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

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

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

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

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

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

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

SIGNATURE

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

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790

01 FC:1806 180.00 DA

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

DM_US 32511456-1.077580.0151

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

Privacy Act Statement

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

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

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

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

Privacy Act Statement

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

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

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

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

Doc Code: TRAN.LET
Document Description: Transmittal Letter

13336790 - GAU: 2453

OPAP MAR 2 3 2012 PATENT & TRADEMARK OFFICE

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)
Total Number of Pages in This Submission	52

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ____________
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature	[signature]		
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

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

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): ____________

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

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

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims ______ - 20 or HP = Extra Claims ______ x Fee ($) ______ = Fee Paid ($) ______

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims ______ - 3 or HP = Extra Claims ______ x Fee ($) ______ = Fee Paid ($) ______

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims: Fee ($) ______ Fee Paid ($) ______

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ______ - 100 = Extra Sheets ______ / 50 = Number of each additional 50 or fraction thereof ______ (round up to a whole number) x Fee ($) ______ = Fee Paid ($) ______

4. OTHER FEE(S)

Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) ______

Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee $180.00

SUBMITTED BY

Signature	/Toby H. Kusmer/	Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OPAP MAR 2 3 2012 IAP23 PATENT & TRADEMARK OFFICE

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

U.S. PATENTS

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

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

/Krisna Lim/ 07/20/2012

13336790 GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. 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/ 07/20/2012

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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/ 07/20/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

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

/Krisna Lim/ 01/20/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/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/ 04/20/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

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

/Krisna Lim/ 07/20/2012

13336790 - GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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/19970620031945/www.aventail.com/educate/whitepaper/sockswp.html~~	
	D249	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	~~D250~~	~~Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing~~	
	D251	Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	D252	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	D253	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	D254	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	
	D255	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D274	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D275	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D276	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D277	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D278	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D279	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D280	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	
	D281	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	D282	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	D283	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	D284	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	D292	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages. 04/25/2001	
	D293	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages.	10/29/1999
	D294	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages.	10/29/1999
	D295	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D296	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D297	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D298	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

13336790 - GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO		Complete if Known
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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).	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D617	Exhibit Y6: Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC1035").	
	D618	Exhibit Y8: Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997.	
	D619	Exhibit Y8: Woodbum, 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/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D640	Exhibit D-4; Yinger; U.S. Patent 5,960,204 to Yinger et al., "System and Method for Installing Applications on a Computer on an as needed basis, Filed on October 28, 1996 and Issued September 28, 1999	
	D641	Exhibit D-8; Barlow; U.S. Patent 5,204,961 to Barlow, "Computer Network Operating with Multilevel Hierarchical Security with Selectable Common Trust Realms and Corresponding Security Protocols," Filed on June 25, 1990 and Issued April 20, 1993	
	D642	Exhibit D-12; RFC 1122, Braden, "Requirements for Internet Hosts – Communication Layers," RFC 1122 (Oct. 1989)	
	D643	Exhibit D-13; RFC 791; Information Sciences Institute, "Intemet 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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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]	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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"	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/

07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

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

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	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	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

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

07/20/2012

/Krisna Lim/

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

Subst. for form 1449/PTO

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

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

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

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country 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.	
	D1201	Exhibit A-1, Kiuchi[1] vs. Claims of the '135 Patent[2]	
	D1202	Exhibit B-1, Kiuchi[1] vs. Claims of the '211 Patent[2]	
	D1203	Exhibit C-1, Kiuchi[1] vs. Claims of the '504 Patent[2]	
	D1204	Exhibit D, Materials Considered	
	D1205	Exhibit E, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1206	Exhibit F, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1207	Exhibit G, Opening Expert Report of Dr. Stuart Stubblebine Regarding Invalidity of the '135, '211, and '504 Patents	

/Krisna Lim/ 07/20/2012

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

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	**13/336,790**
				Filing Date	**12-23-2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Krisna Lim**
				Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

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

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

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

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

[ ] None

SIGNATURE

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

/Toby H Kusmer/

Date: 6/1/12

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

DM_US 35546776-1.077580.0151

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

US006502135C1

(12) **INTER PARTES REEXAMINATION CERTIFICATE** (0271st)

United States Patent

Munger et al.

(10) **Number:** **US 6,502,135 C1**

(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

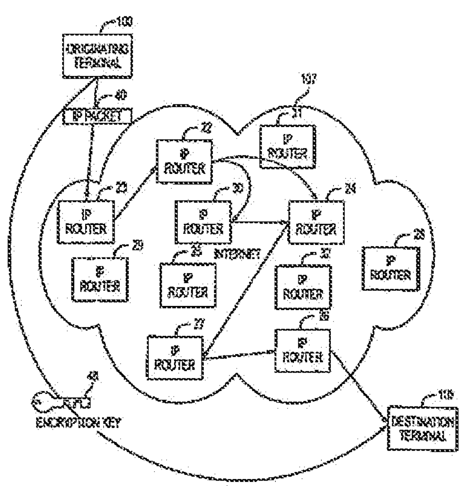
Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/draft302.txt on Feb. 4, 2002, 56 pages.

(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

VX00088635

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 WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet).
Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) available at http://msdn2.microsoft.com/enus/library/ms811078 (printer).aspx (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).

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. Matehrs 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.

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:

(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

Dft Apple's
Trial Exhibit
DX-A 62
6:10-CV-00417-LED

0 7107319

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

January 15, 2008

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF:

U.S. PATENT: *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

T. Lawrence

T. LAWRENCE
Certifying Officer

US006502135B1

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

(10) **Patent No.: US 6,502,135 B1**
(45) **Date of Patent: Dec. 31, 2002**

(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: **Science Applications International Corporation**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/504,783**

(22) Filed: **Feb. 15, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(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.**[7] **G06F 15/173**
(52) **U.S. Cl.** **709/225**; 709/229; 709/245
(58) **Field of Search** 709/249, 223, 709/225, 229, 245; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE publication, 1996, pp. 963–967.

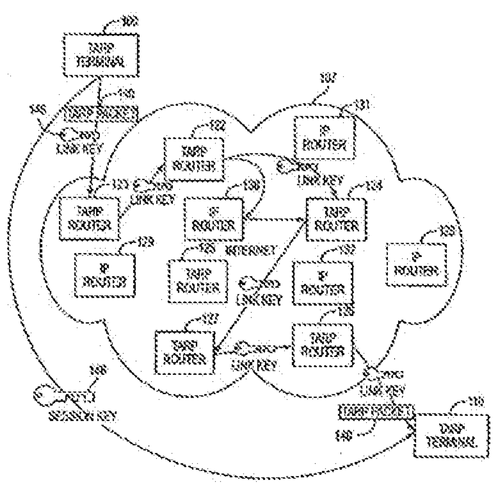
(List continued on next page.)

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

(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.

17 Claims, 35 Drawing Sheets



U.S. PATENT DOCUMENTS

5,588,060	A		12/1996	Aziz	
5,689,566	A		11/1997	Nguyen	
5,796,942	A		8/1998	Esbensen	
5,805,801	A		9/1998	Holloway et al.	
5,842,040	A		11/1998	Hughes et al.	
5,878,231	A	*	3/1999	Baehr et al.	709/243
5,892,903	A		4/1999	Klaus	
5,898,830	A	*	4/1999	Wesinger et al.	709/225
5,905,859	A		5/1999	Holloway et al.	
6,006,259	A		12/1999	Adelman et al.	
6,016,318	A	*	1/2000	Tomoike	370/338
6,052,788	A		4/2000	Wesinger, Jr. et al.	
6,079,020	A	*	6/2000	Liu	713/201
6,119,171	A		9/2000	Alkhatib	
6,178,505	B1	*	1/2001	Schneider et al.	713/168
6,226,751	B1	*	5/2001	Arrow et al.	370/351
6,243,749	B1		6/2001	Sitaraman et al.	
6,286,047	B1	*	9/2001	Ramanathan et al.	345/733
6,330,562	B1	*	12/2001	Boden et al.	707/10
6,332,158	B1	*	12/2001	Risley et al.	709/219
6,353,614	B1	*	3/2002	Borella et al.	370/389

OTHER PUBLICATIONS

Linux FreeS/WAN Index File, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 pages.

J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.

Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan/org/freeswan_trees/freeswan-1.3/doc/glossary.html on Feb. 21, 2002, 25 pages.

Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ssl3/draft302.txt on Feb. 4, 2002, 56 pages.

Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs—Research), "Crowds: Anonymity for Web Transactions", pp. 1–23.

Dolev, Shlomi and Ostrovsky, Rafail, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.

Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82–94.

Shree Murthy et al., "Congestion-Oriented Shortest Multipath Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028–1036.

Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1–14.

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

Search Report (dated Jun. 28, 2002), International Application No. PCT/US01/13261.

Donald E. Eastlake, "Domain Name System Security Extensions", DNS Security Working Group, Apr. 1998, 51 pages.

D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278–297 and pp. 351–375.

P. Srisuresh et al., "DNS extensions to Network Address Translators", Jul. 1998, 27 pages.

Laurie Wells, "Security Icon", Oct. 19, 1998, 1 page.

W. Stallings, "Cryptography And Network Security", 2nd Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399–440.

W. Stallings, "New Cryptography and Network Security Book", Jun. 8, 1998, 3 pages.

* cited by examiner

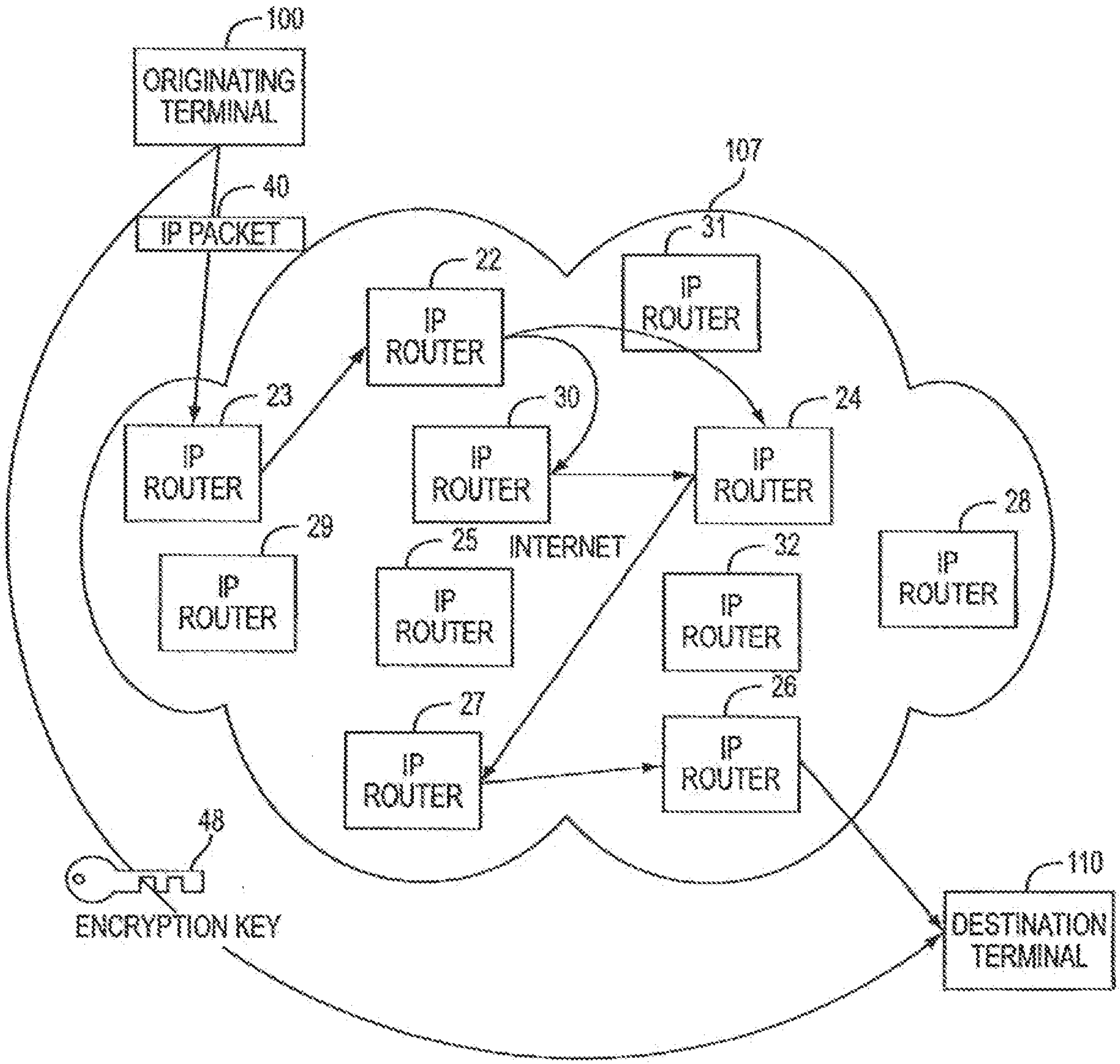

100
ORIGINATING TERMINAL
40
IP PACKET
107
31
IP ROUTER
22
IP ROUTER
23
IP ROUTER
30
IP ROUTER
24
IP ROUTER
29
IP ROUTER
25
IP ROUTER
INTERNET
32
IP ROUTER
28
IP ROUTER
27
IP ROUTER
26
IP ROUTER
48
ENCRYPTION KEY
110
DESTINATION TERMINAL

FIG. 1

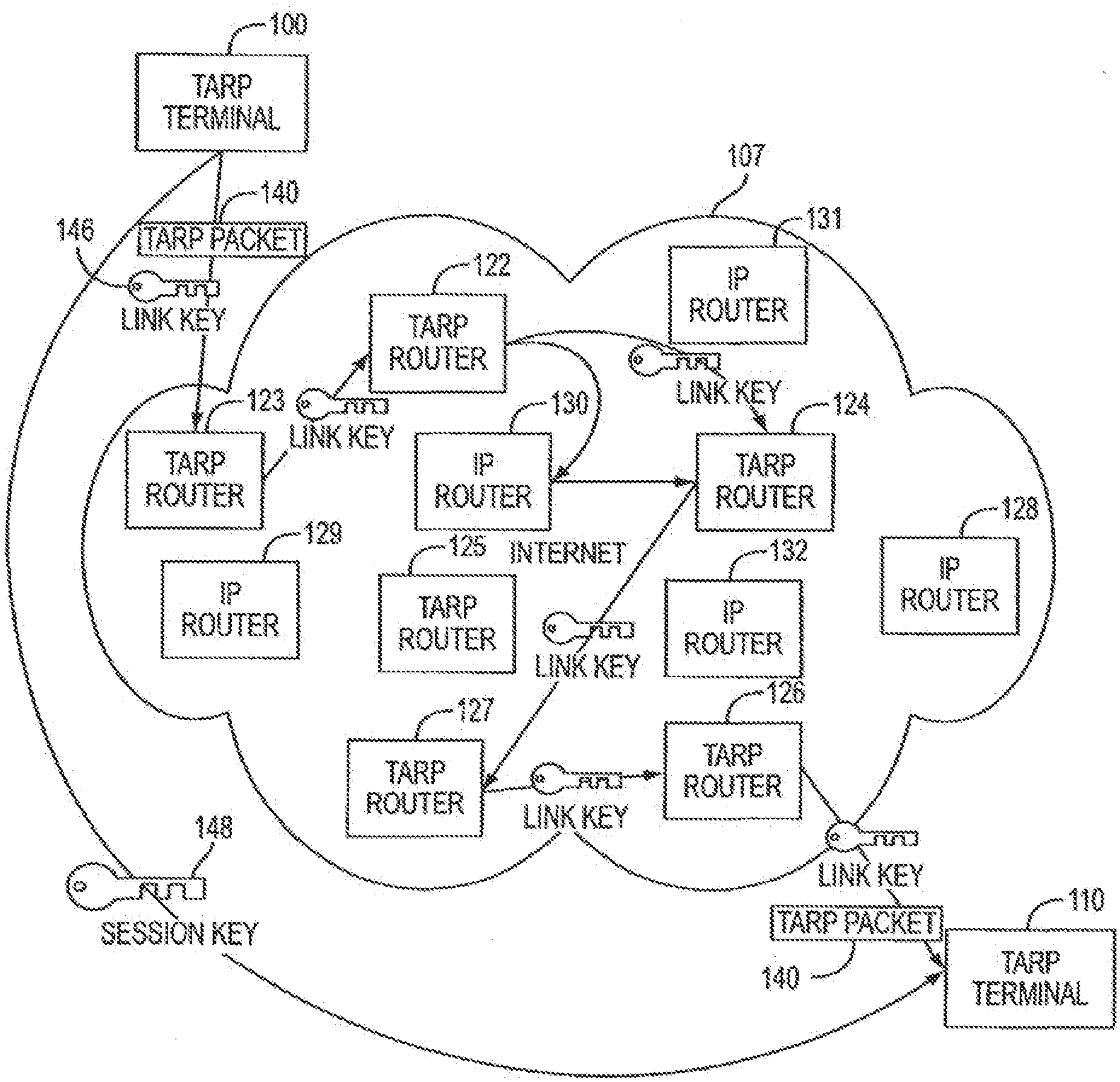
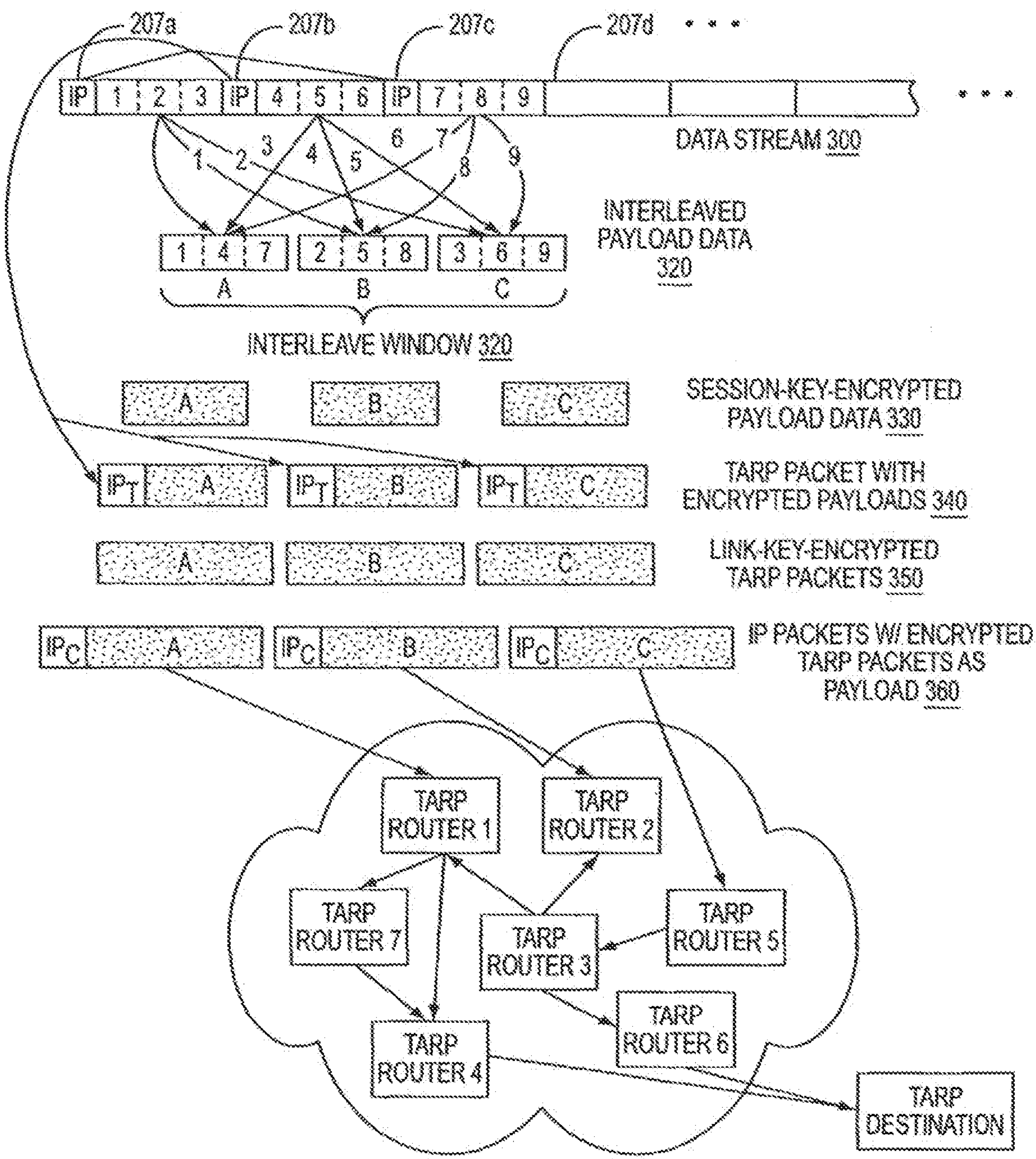

100
TARP TERMINAL
107
140
TARP PACKET
146
LINK KEY
122
TARP ROUTER
131
IP ROUTER
123
TARP ROUTER
LINK KEY
130
IP ROUTER
LINK KEY
124
TARP ROUTER
129
IP ROUTER
125
TARP ROUTER
INTERNET
132
IP ROUTER
128
IP ROUTER
LINK KEY
127
TARP ROUTER
126
TARP ROUTER
LINK KEY
LINK KEY
148
SESSION KEY
TARP PACKET
110
TARP TERMINAL
140

FIG. 2



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

FIG. 3A

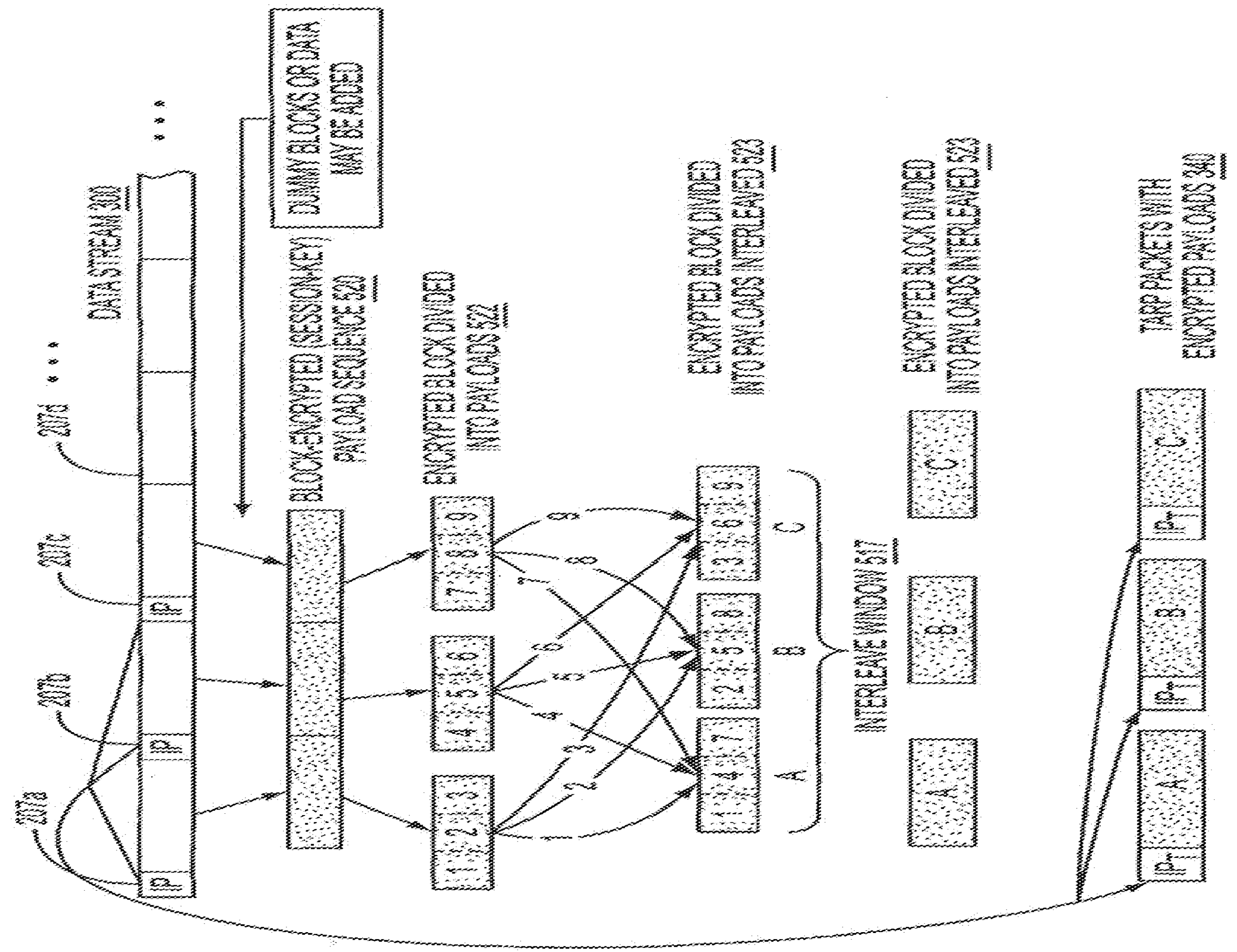

207a
207b
207c
207d
DATA STREAM 300
IP
IP
IP
DUMMY BLOCKS OR DATA MAY BE ADDED
BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE 520
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS 522
1 2 3
4 5 6
7 8 9
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED 523
1 4 7
2 5 8
3 6 9
A
B
C
INTERLEAVE WINDOW 517
ENCRYPTED BLOCK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

FIG. 3B

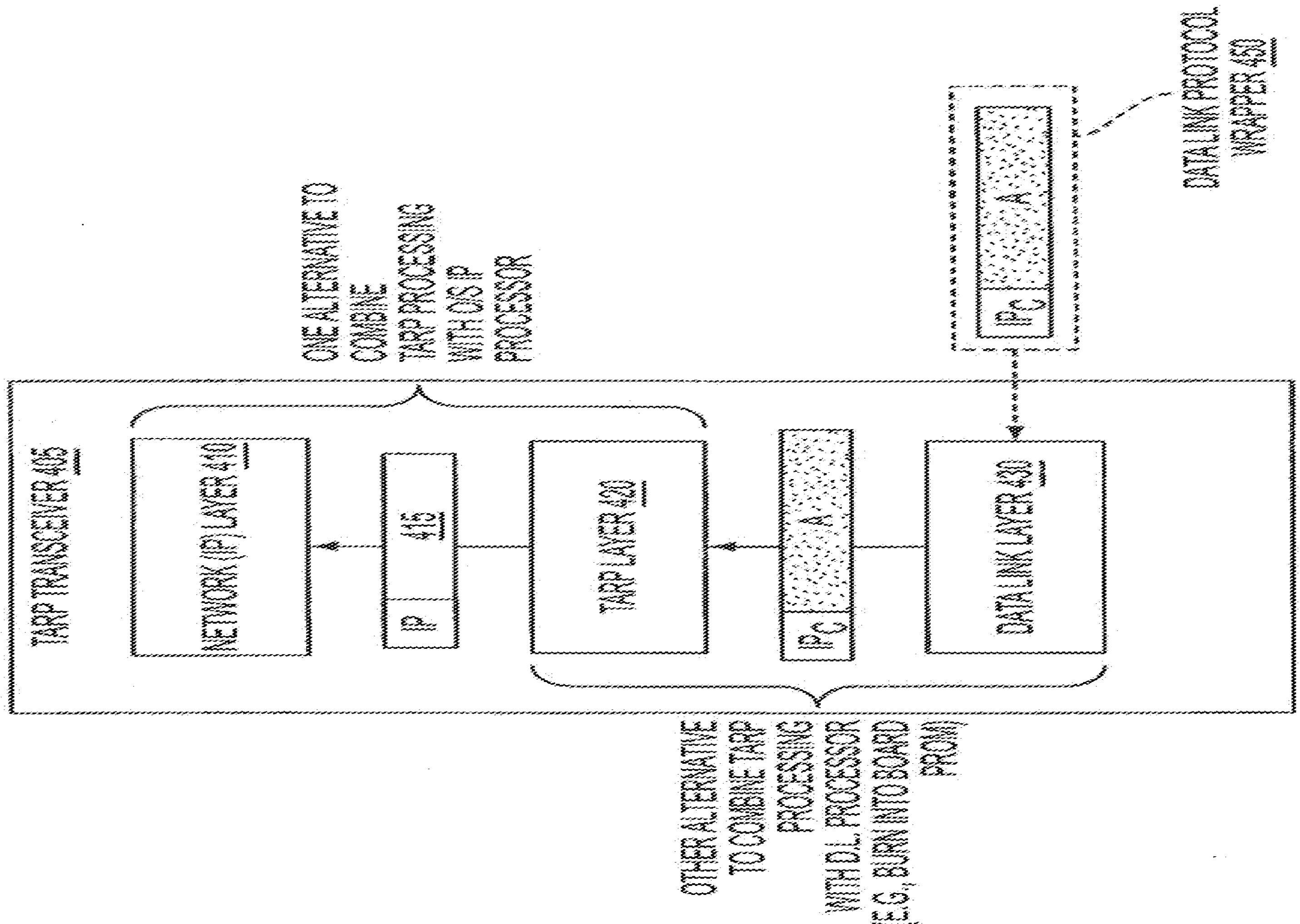

TARP TRANSCEIVER 405
NETWORK (IP) LAYER 410
IP
415
TARP LAYER 420
IP_C
A
DATA LINK LAYER 430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (E.G., BURN INTO BOARD PROM)
DATA LINK PROTOCOL WRAPPER 450

FIG. 4

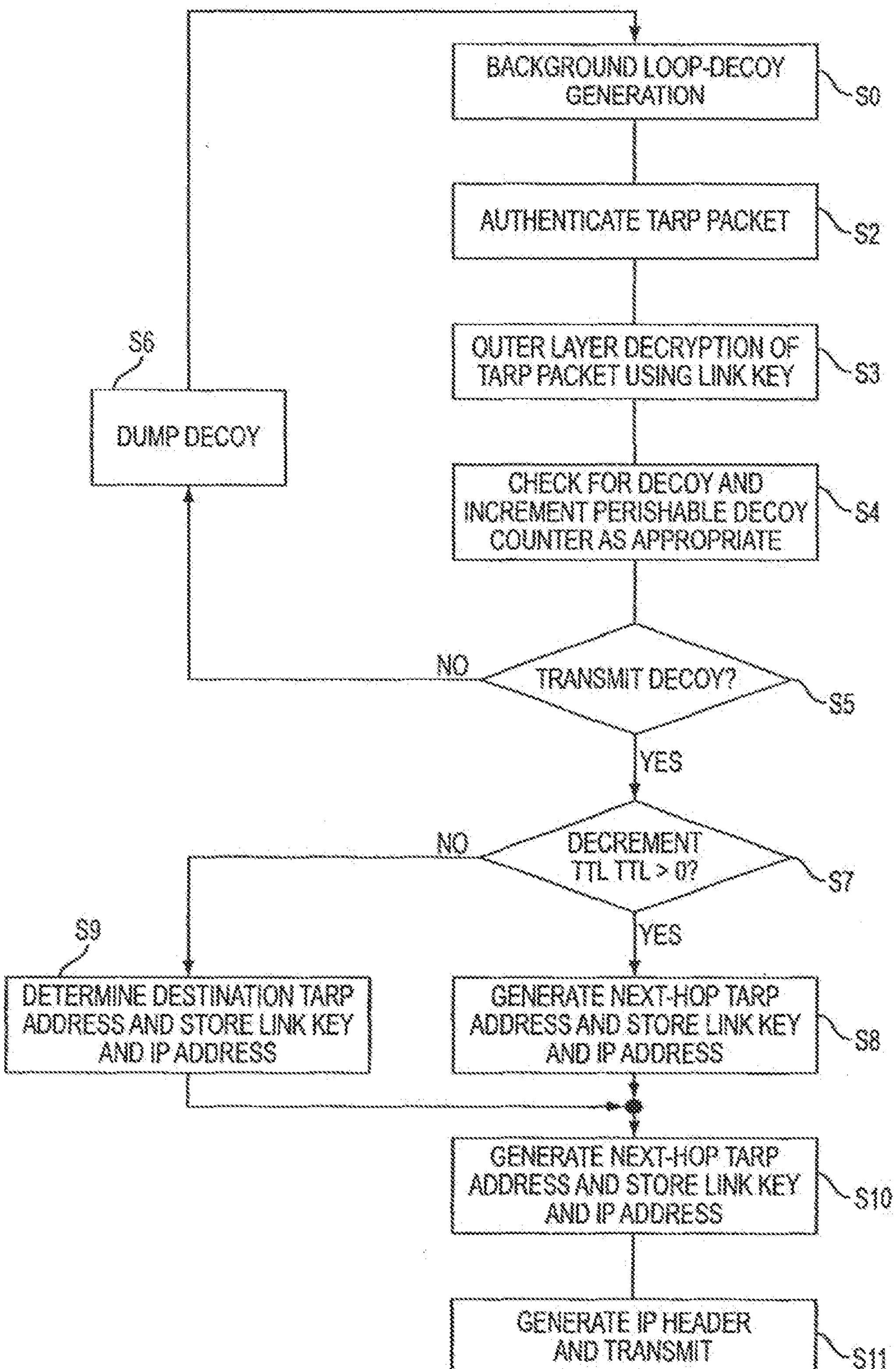

BACKGROUND LOOP-DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
S6
DUMP DECOY
NO
TRANSMIT DECOY?
S5
YES
NO
DECREMENT TTL TTL > 0?
S7
YES
S9
DETERMINE DESTINATION TARP ADDRESS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

FIG. 5

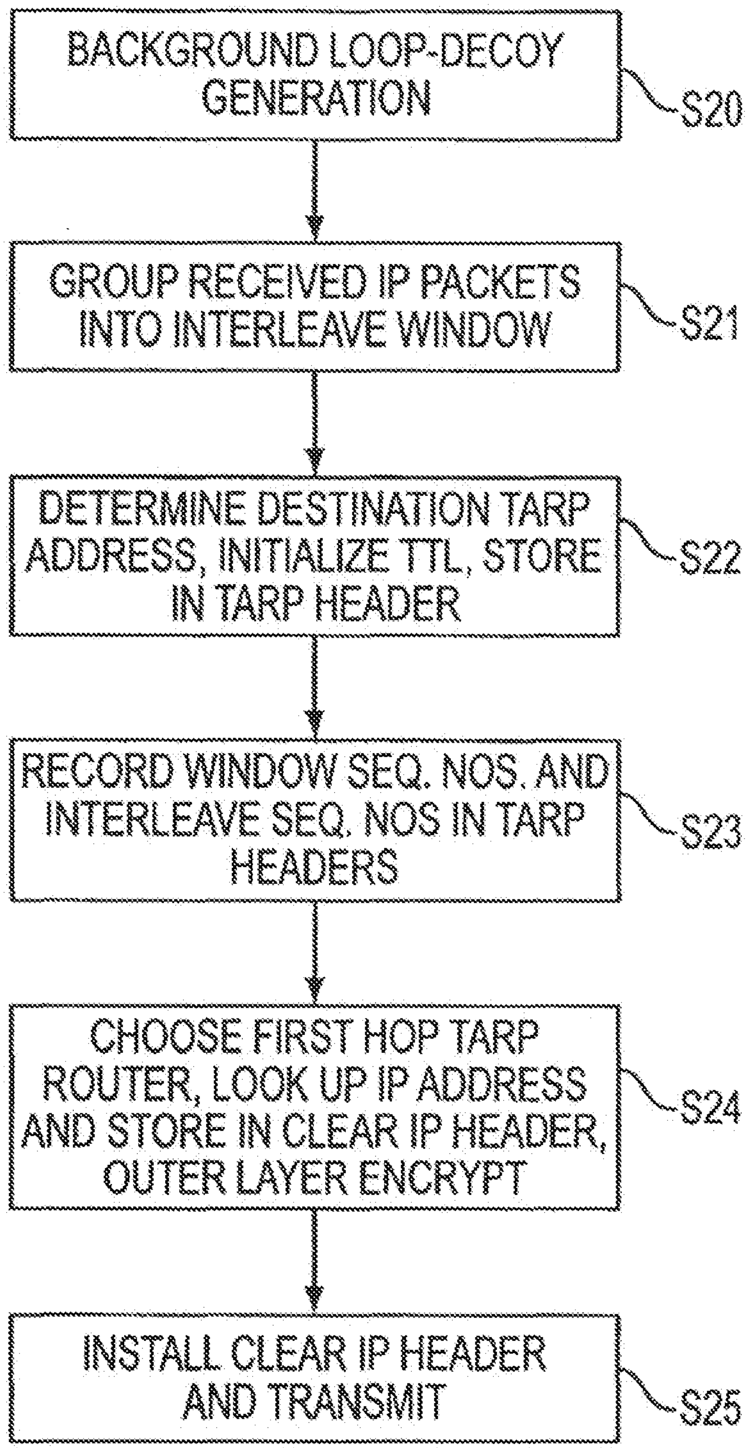

BACKGROUND LOOP-DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR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

FIG. 6

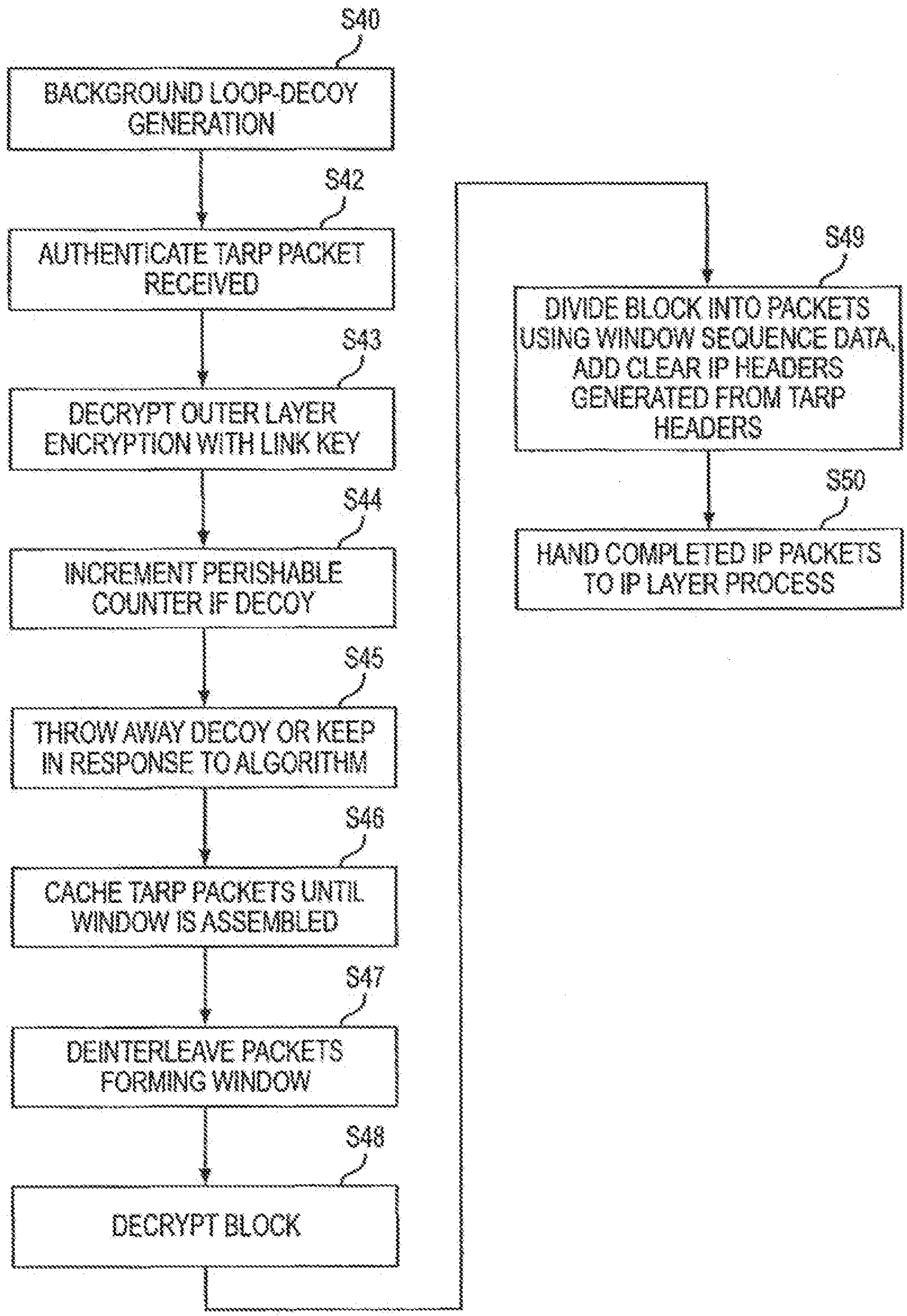

S40
BACKGROUND LOOP-DECOY GENERATION
S42
AUTHENTICATE TARP PACKET RECEIVED
S43
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S44
INCREMENT PERISHABLE COUNTER IF DECOY
S45
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S46
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S47
DEINTERLEAVE PACKETS FORMING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

FIG. 7

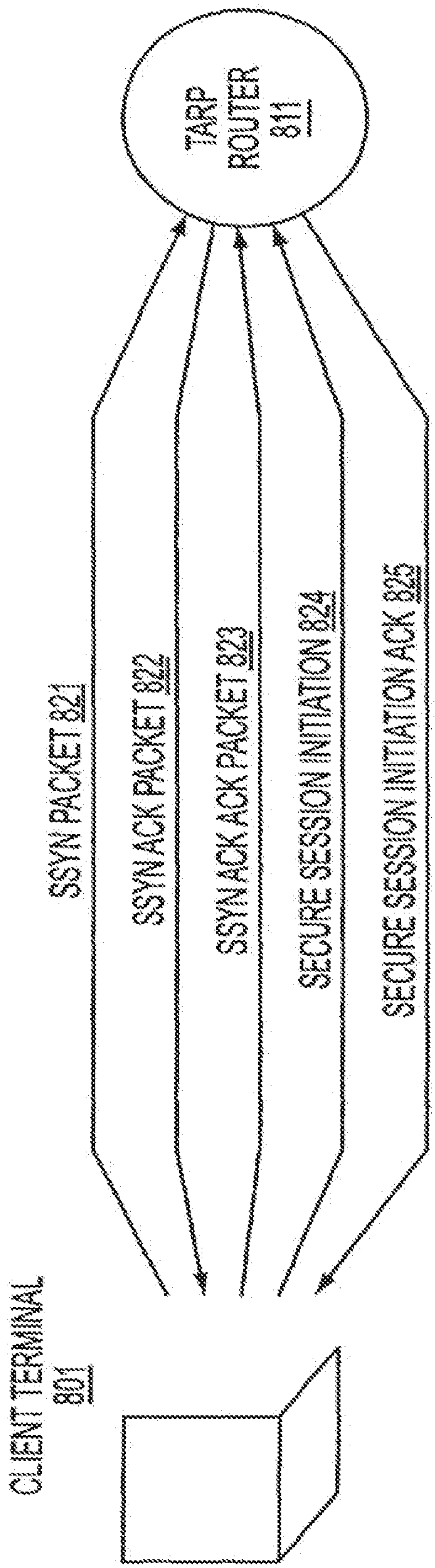
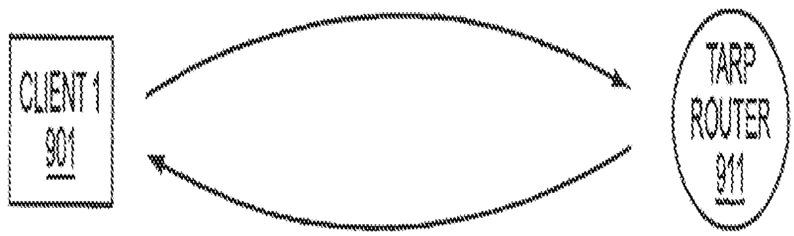

TARP ROUTER 811
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
SECURE SESSION INITIATION 824
SECURE SESSION INITIATION ACK 825
CLIENT TERMINAL 801

FIG. 8



TRANSMIT TABLE 921

131.218.204.98	,	131.218.204.65
131.218.204.221	,	131.218.204.97
131.218.204.139	,	131.218.204.186
131.218.204.12	,	131.218.204.55
.		.
.		.
.		.

RECEIVE TABLE 924

131.218.204.98	,	131.218.204.65
131.218.204.221	,	131.218.204.97
131.218.204.139	,	131.218.204.186
131.218.204.12	,	131.218.204.55
.		.
.		.
.		.

RECEIVE TABLE 922

131.218.204.161	,	131.218.204.89
131.218.204.66	,	131.218.204.212
131.218.204.201	,	131.218.204.127
131.218.204.119	,	131.218.204.49
.		.
.		.
.		.

TRANSMIT TABLE 923

131.218.204.161	,	131.218.204.89
131.218.204.66	,	131.218.204.212
131.218.204.201	,	131.218.204.127
131.218.204.119	,	131.218.204.49
.		.
.		.
.		.

FIG. 9

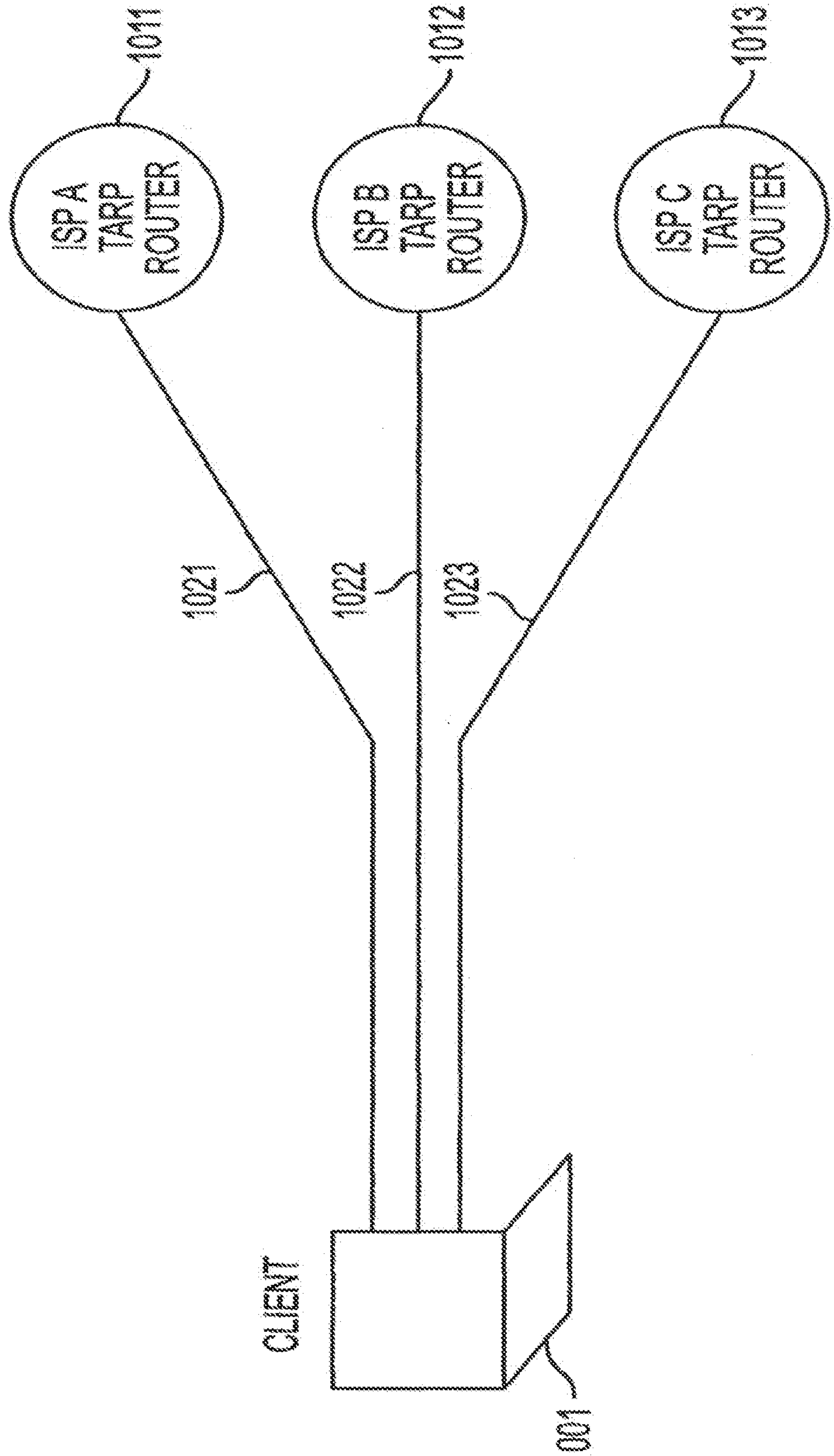

ISP A
TARP
ROUTER
1011
ISP B
TARP
ROUTER
1012
ISP C
TARP
ROUTER
1013
1021
1022
1023
CLIENT
1001

FIG. 10

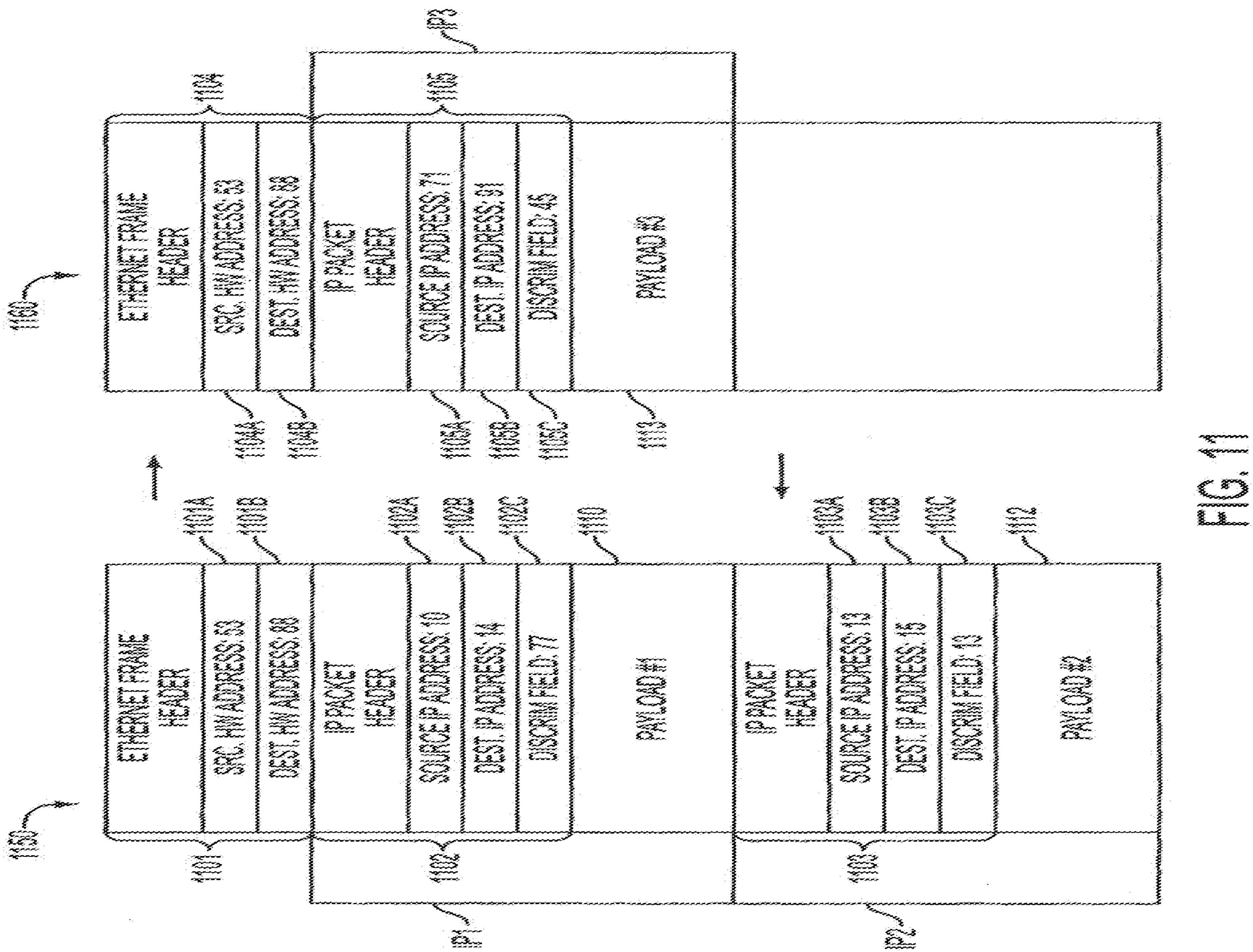
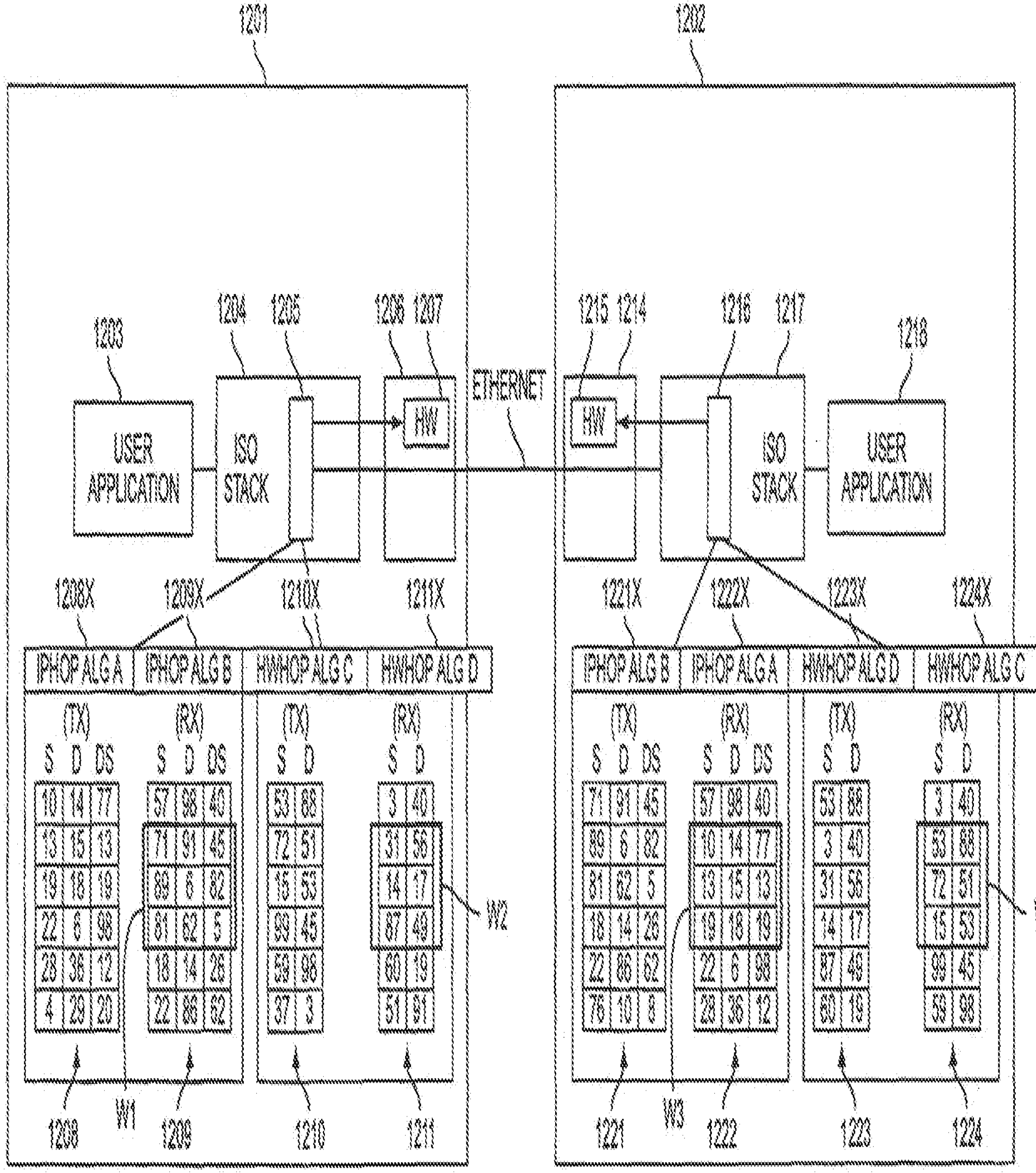

1150
1160
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW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

FIG. 11



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

FIG. 12A

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

FIG. 12B

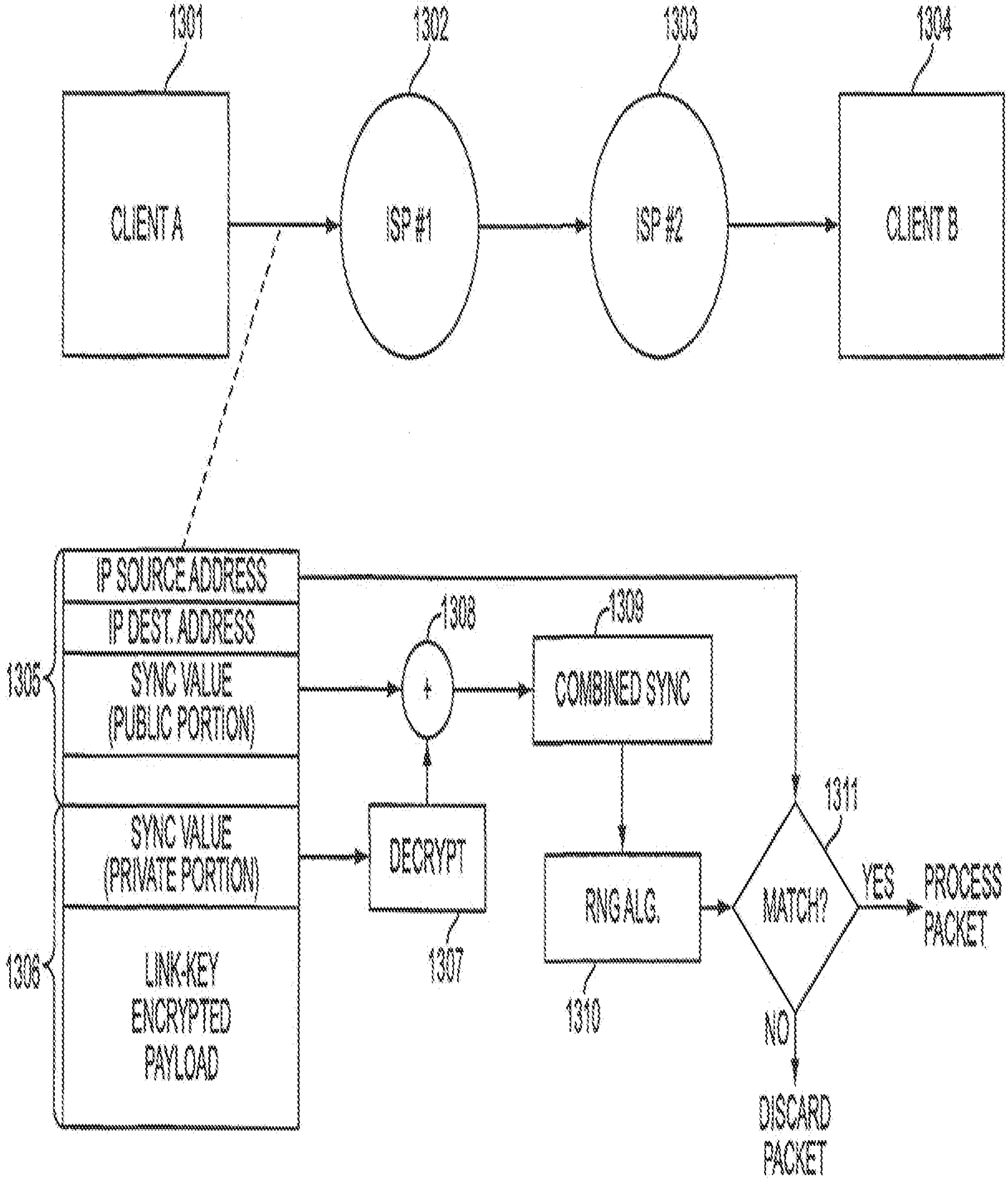

1301
CLIENT A
1302
ISP #1
1303
ISP #2
1304
CLIENT B
1305
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE (PUBLIC PORTION)
1306
SYNC VALUE (PRIVATE PORTION)
LINK-KEY ENCRYPTED PAYLOAD
1307
DECRYPT
1308
+
1309
COMBINED SYNC
1310
RNG ALG.
1311
MATCH?
YES
PROCESS PACKET
NO
DISCARD PACKET

FIG. 13

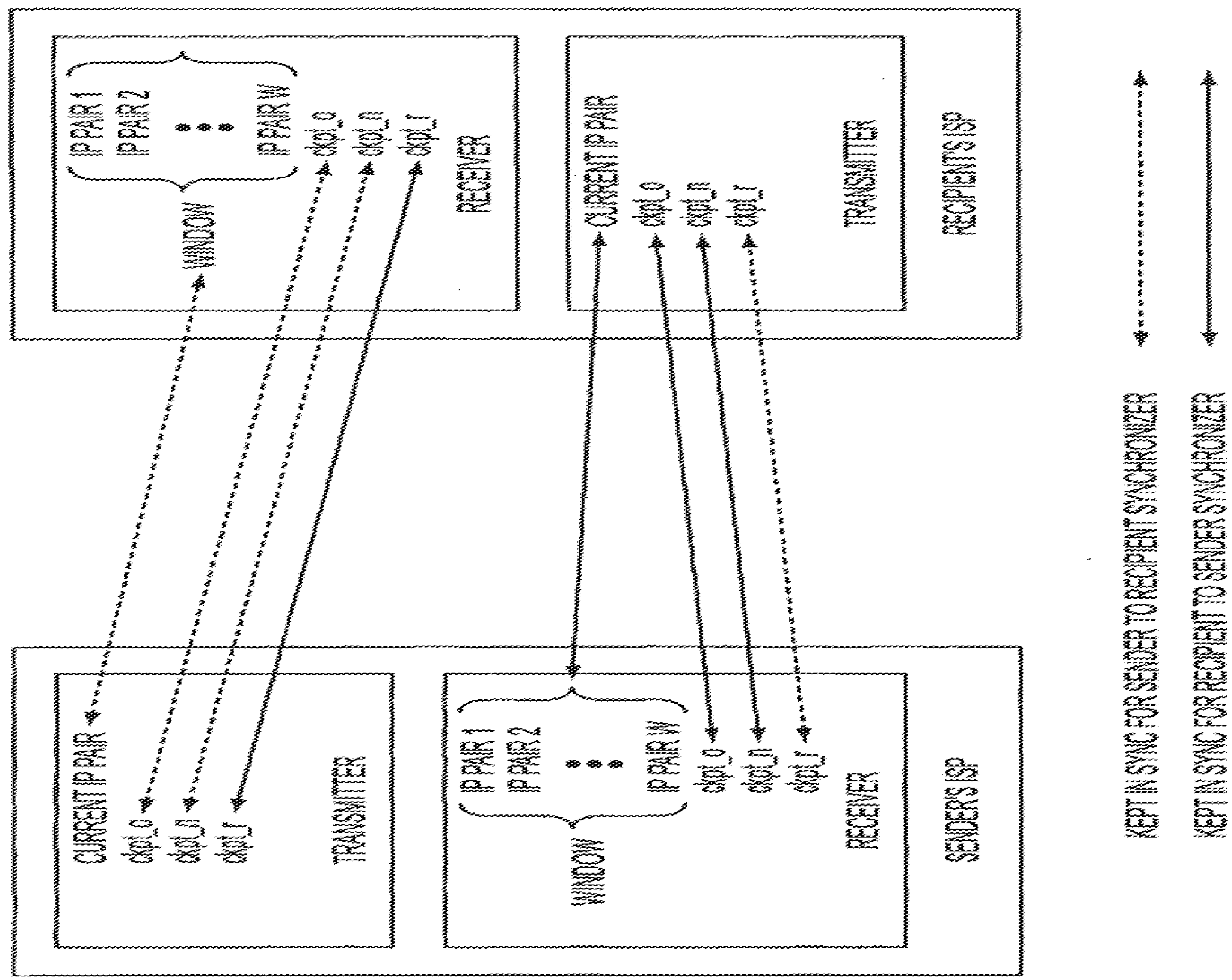

IP PAIR 1
IP PAIR 2
IP PAIR W
WINDOW
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
IP PAIR 1
IP PAIR 2
IP PAIR W
WINDOW
ckpt_o
ckpt_n
ckpt_r
RECEIVER
SENDER'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER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

FIG. 14

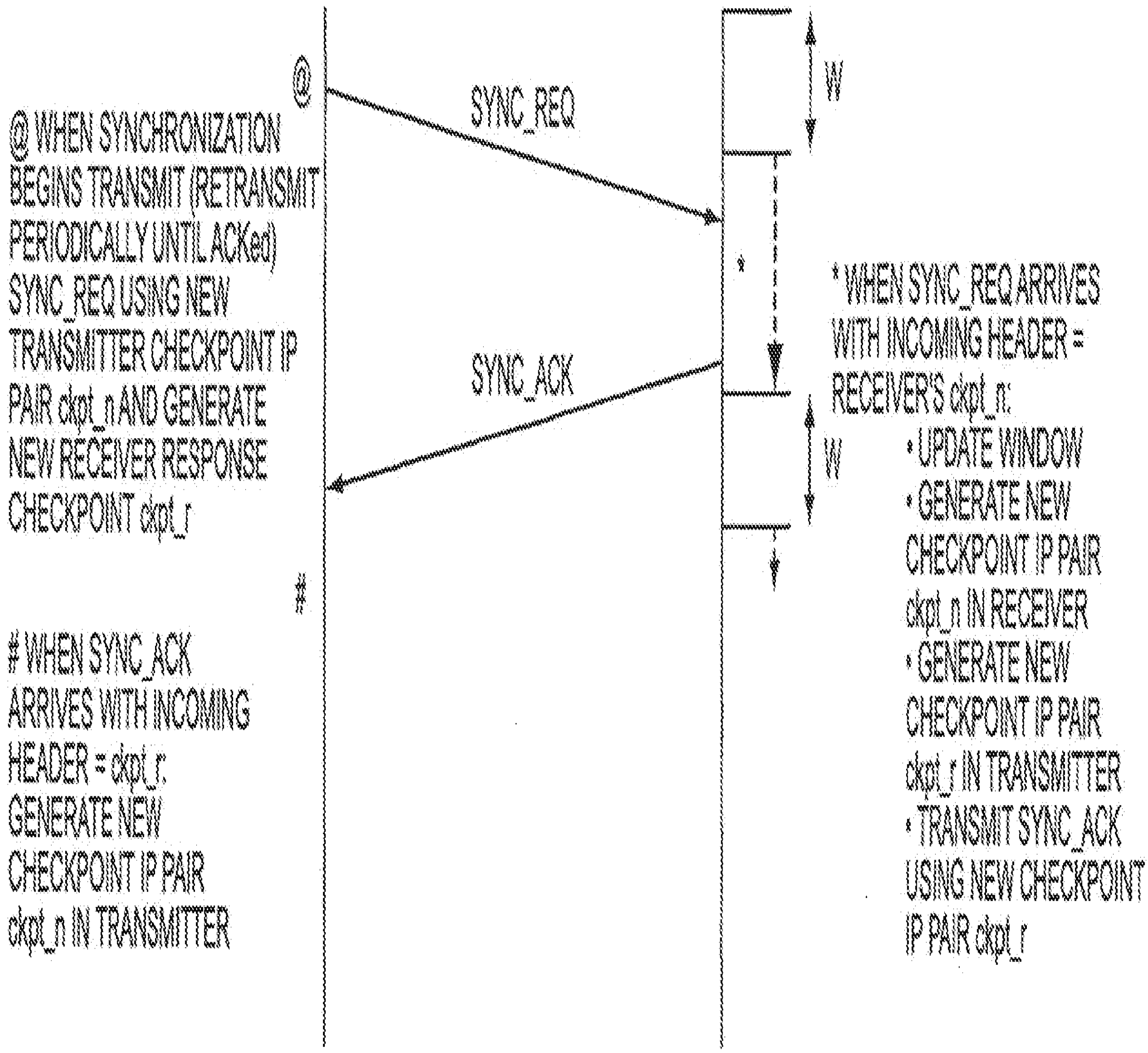

@
SYNC_REQ
SYNC_ACK
W
W
*
#
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
# WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r: GENERATE NEW CHECKPOINT IP PAIR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

FIG. 15

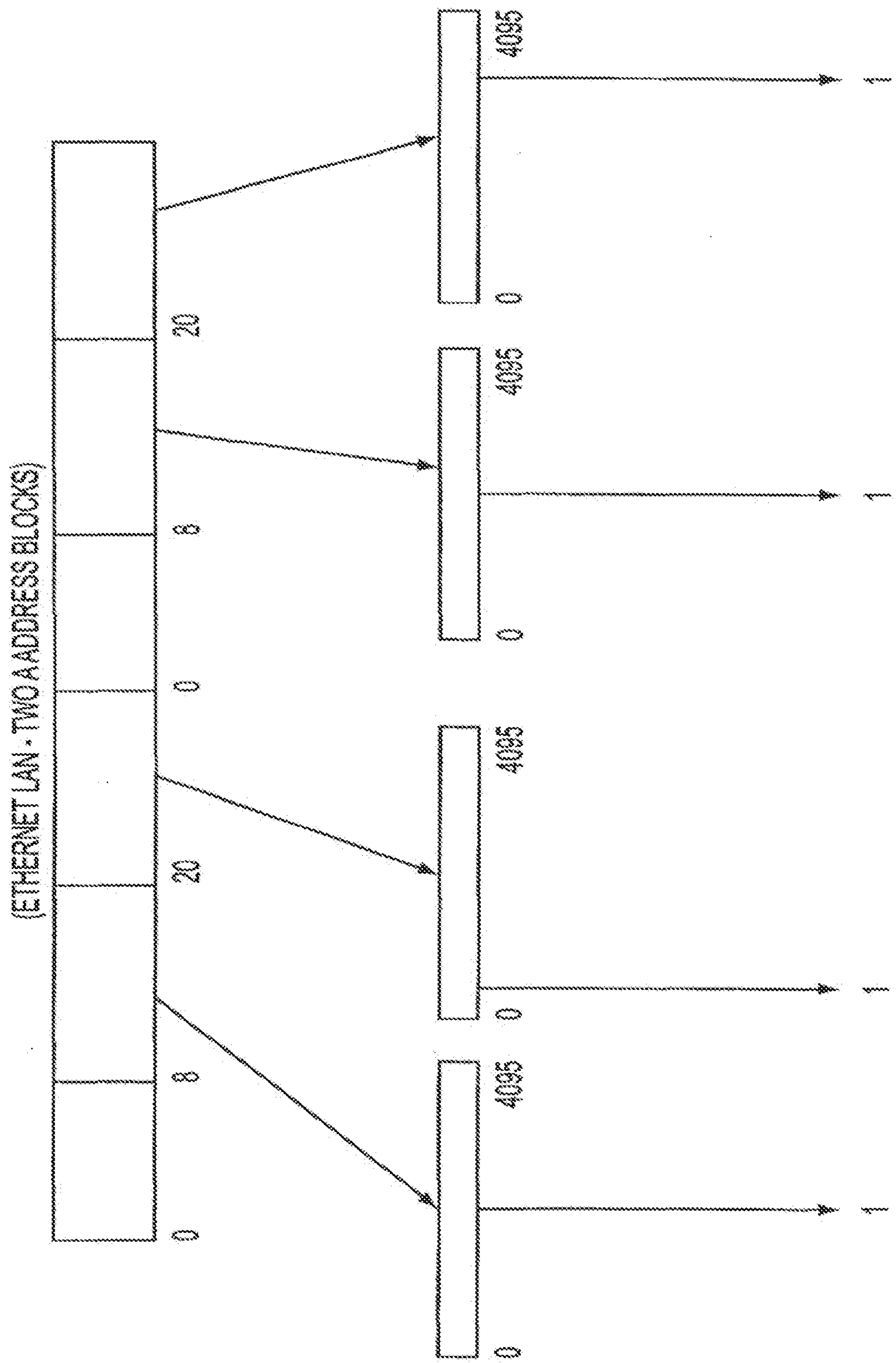


FIG. 16

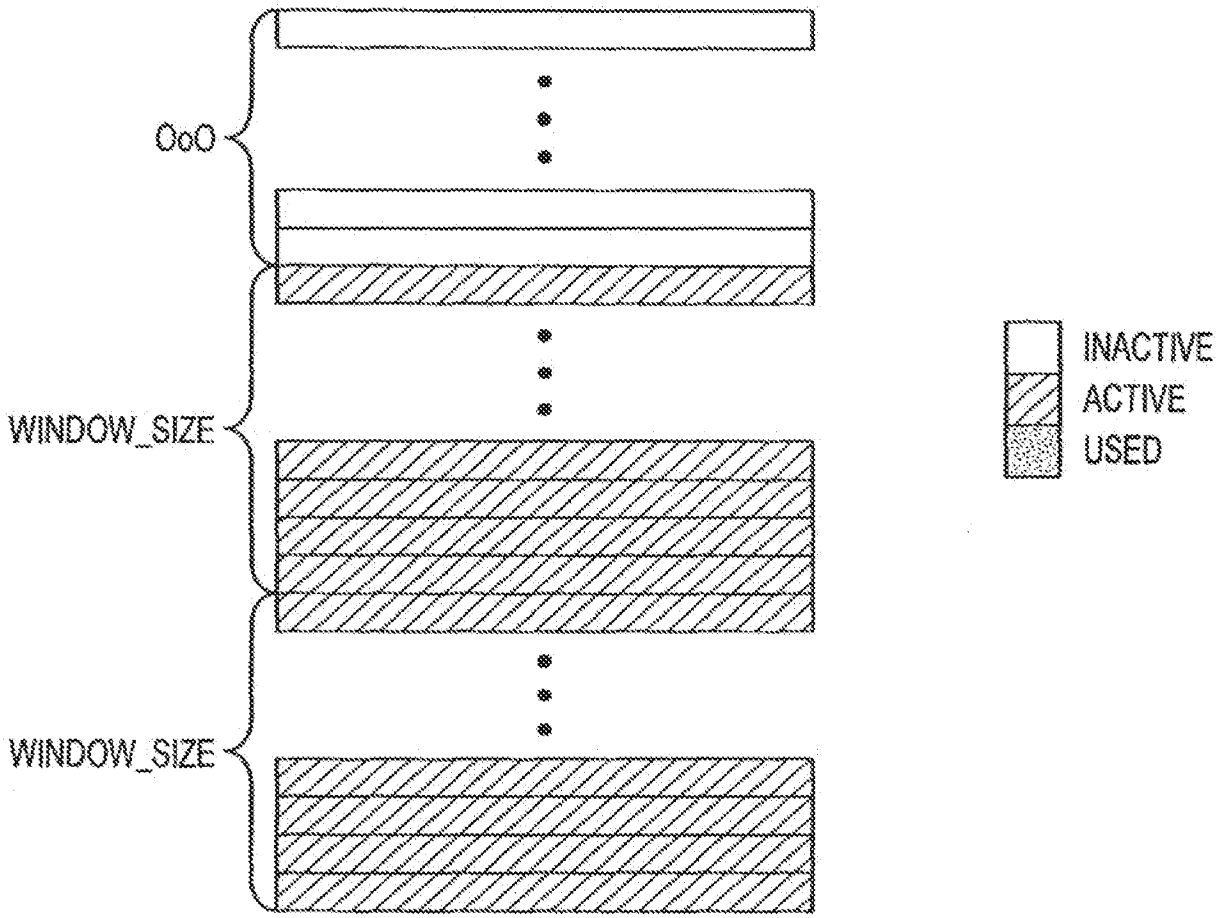


FIG. 17

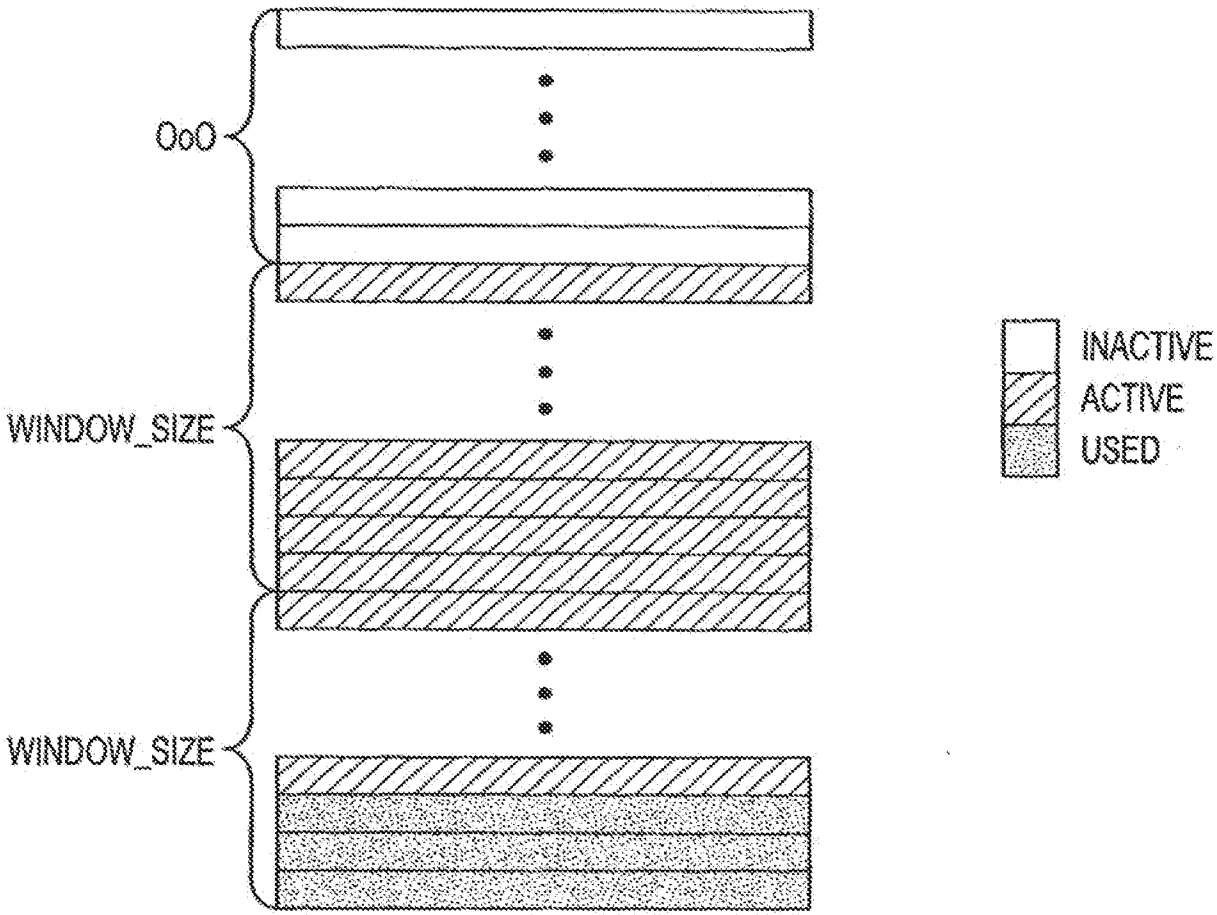


FIG. 18

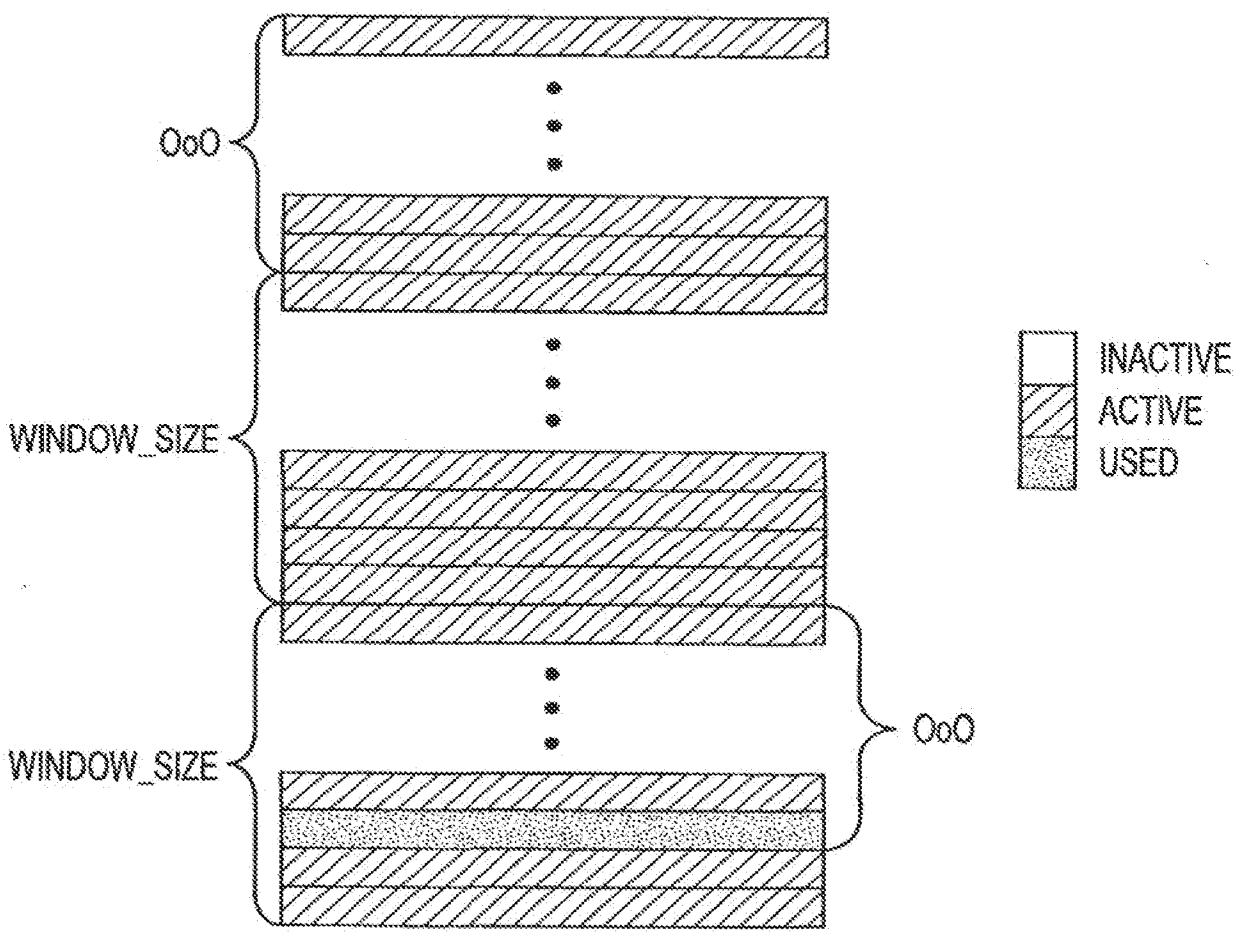
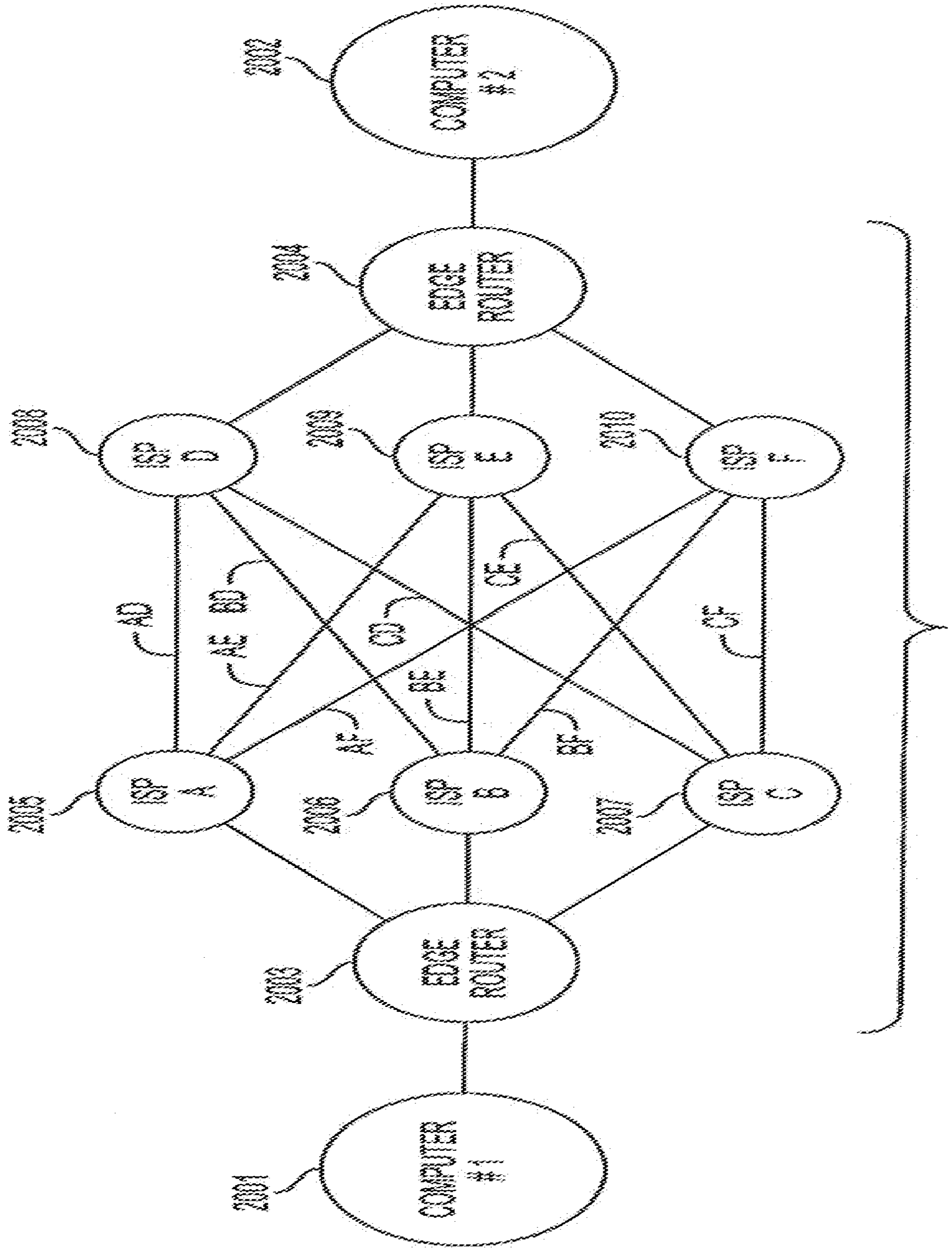


FIG. 19



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

FIG. 20

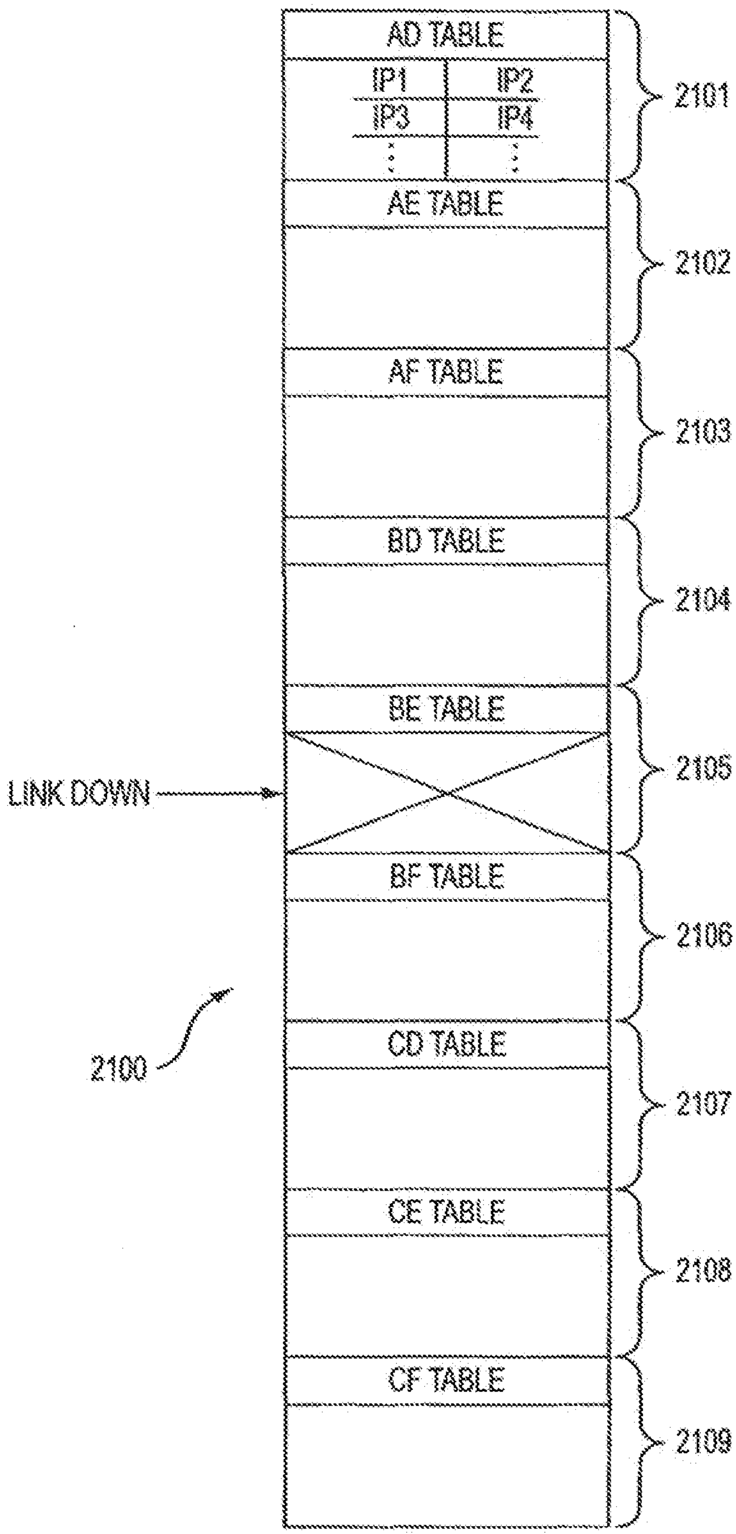
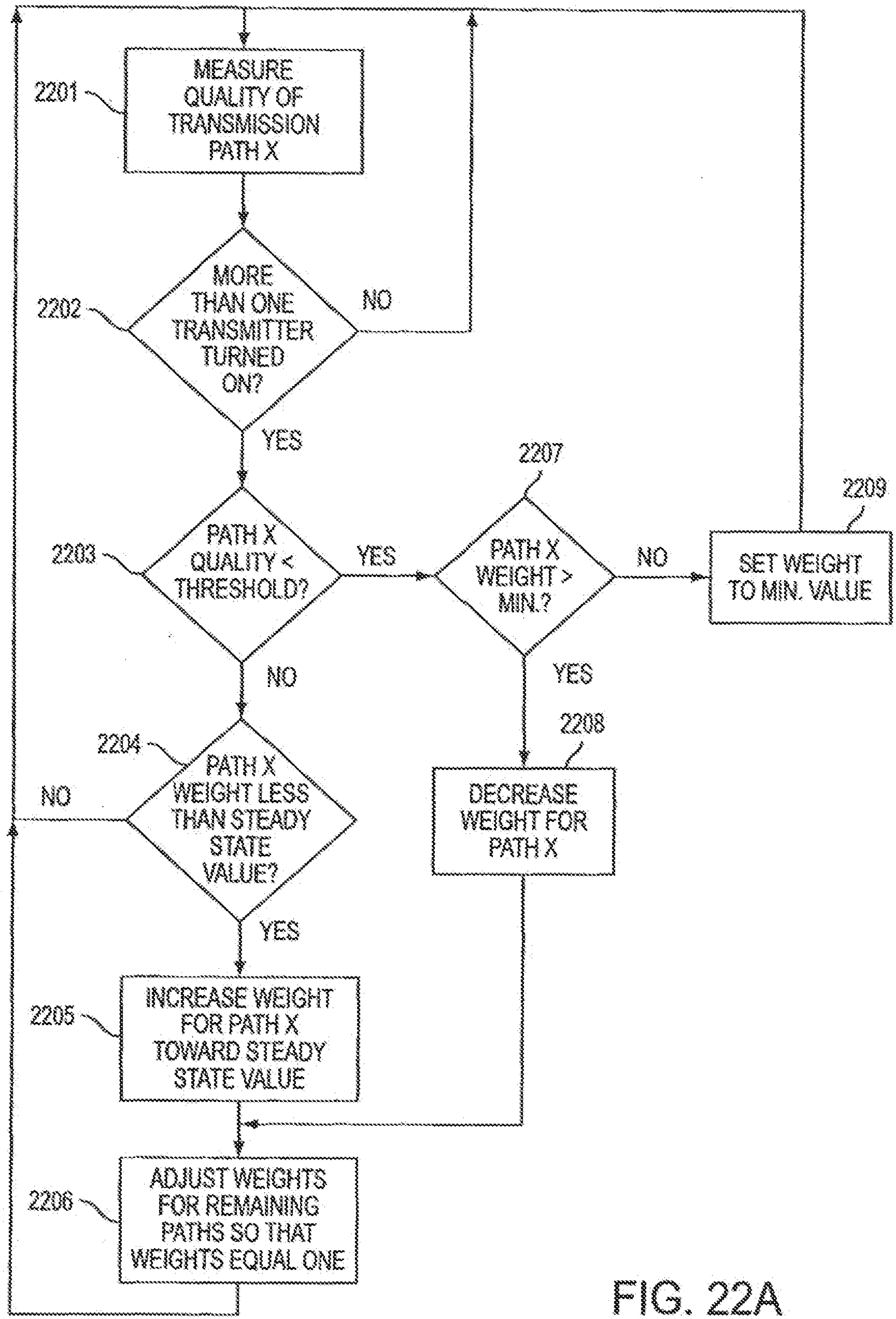

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
LINK DOWN
2105
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

FIG. 21



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

FIG. 22A

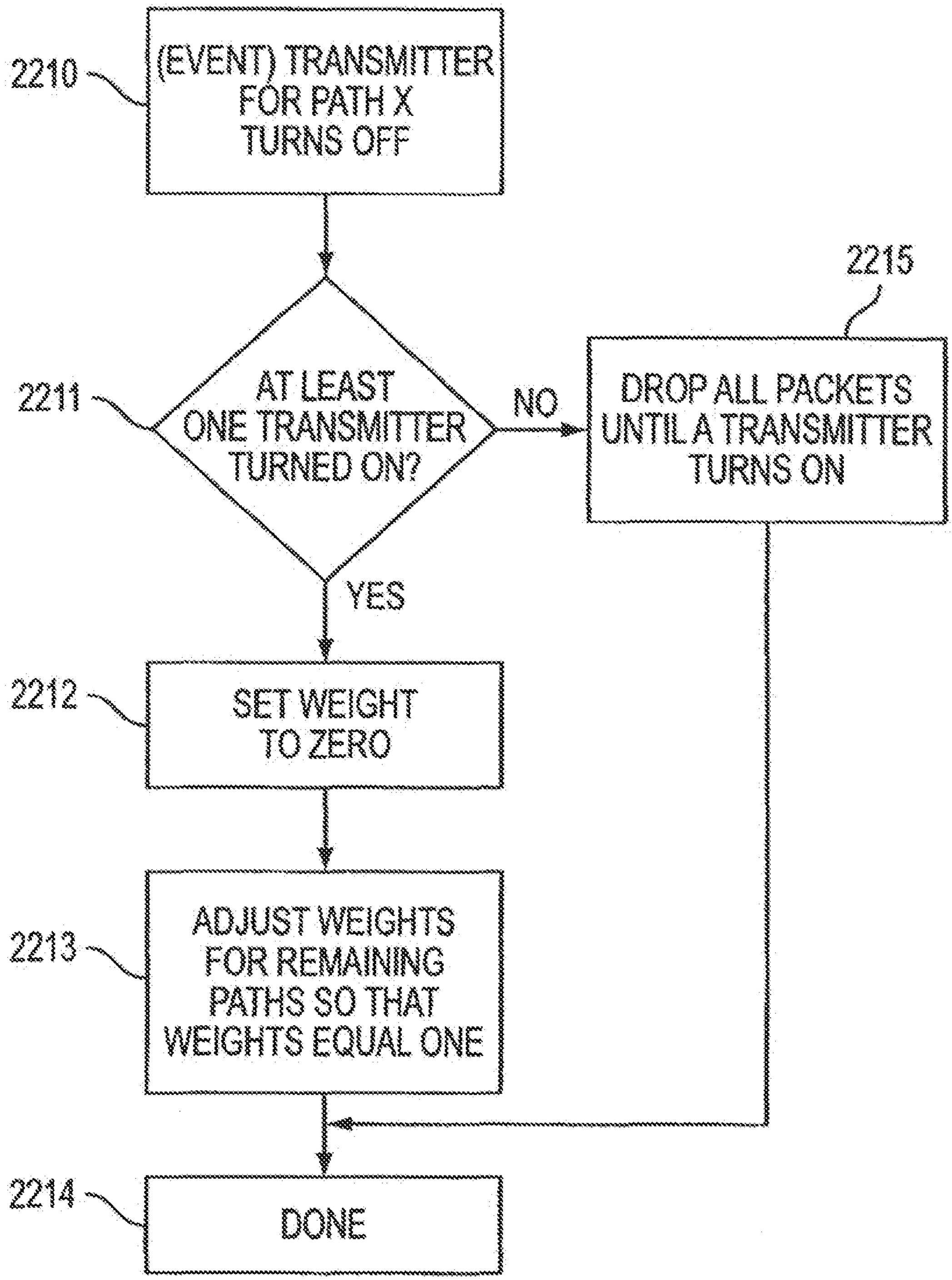

2210
(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2211
AT LEAST ONE TRANSMITTER TURNED ON?
NO
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
YES
2212
SET WEIGHT TO ZERO
2213
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2214
DONE

FIG. 22B

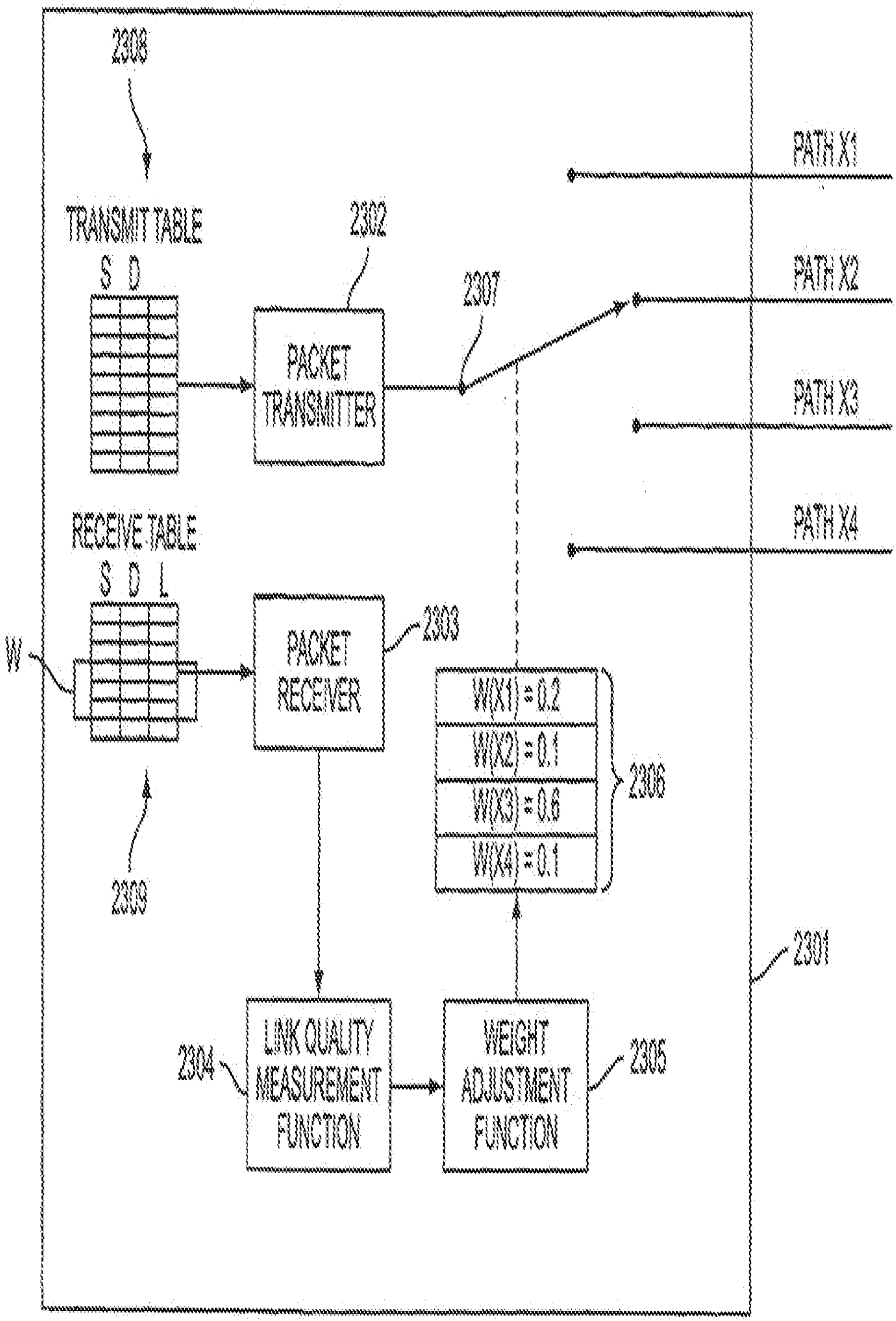

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
W
PACKET RECEIVER
2303
W(X1) = 0.2
W(X2) = 0.1
W(X3) = 0.6
W(X4) = 0.1
2306
2309
2301
LINK QUALITY MEASUREMENT FUNCTION
2304
WEIGHT ADJUSTMENT FUNCTION
2305

FIG. 23

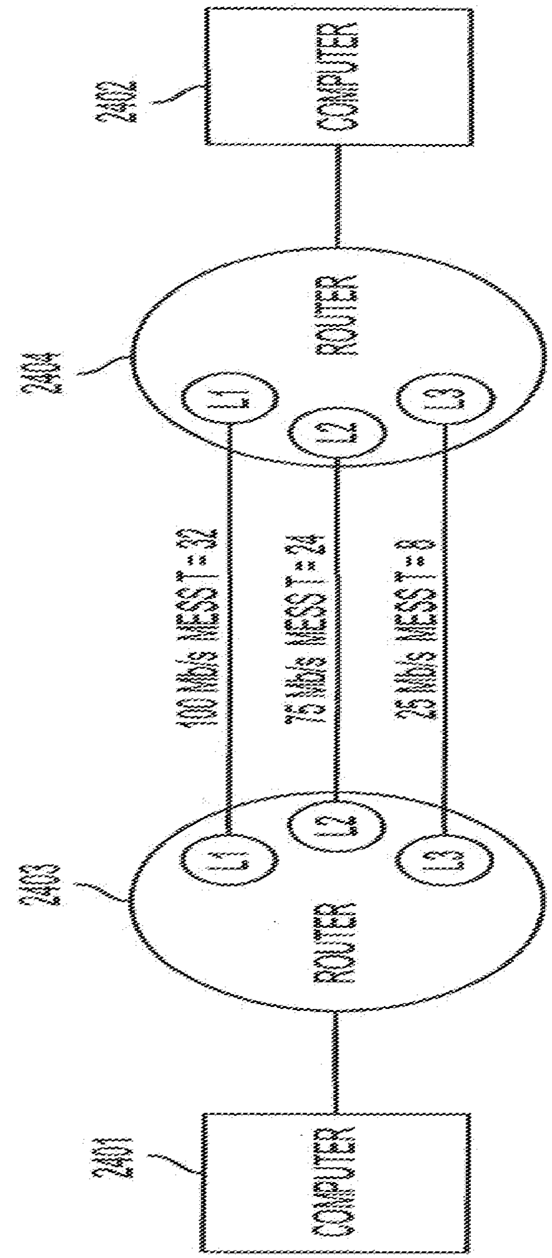

2401
COMPUTER
2403
ROUTER
L1
L2
L3
100 Mb/s MESS T = 32
75 Mb/s MESS T = 24
25 Mb/s MESS T = 8
2404
L1
L2
L3
ROUTER
2402
COMPUTER

FIG. 24

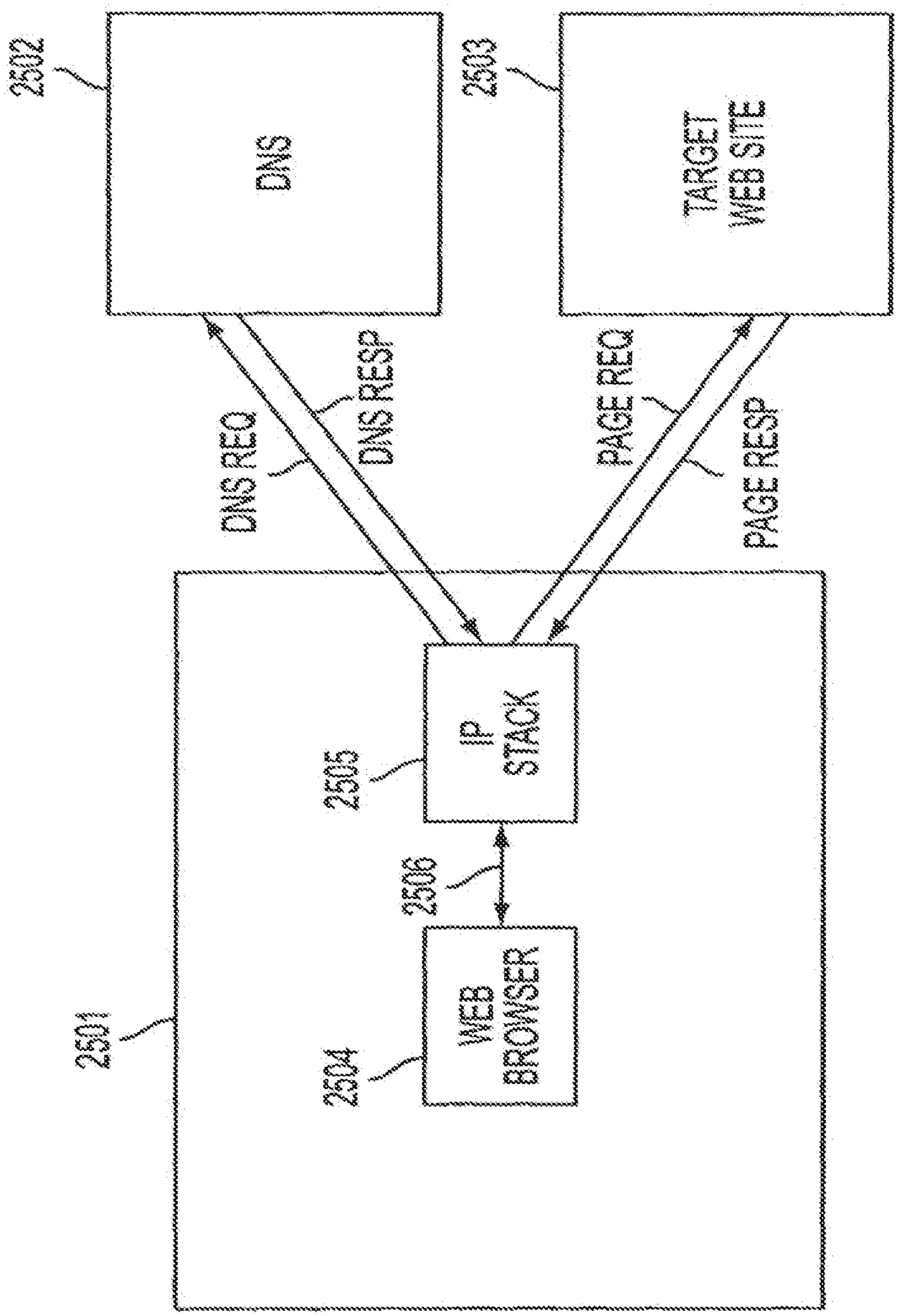


FIG. 25
(PRIOR ART)

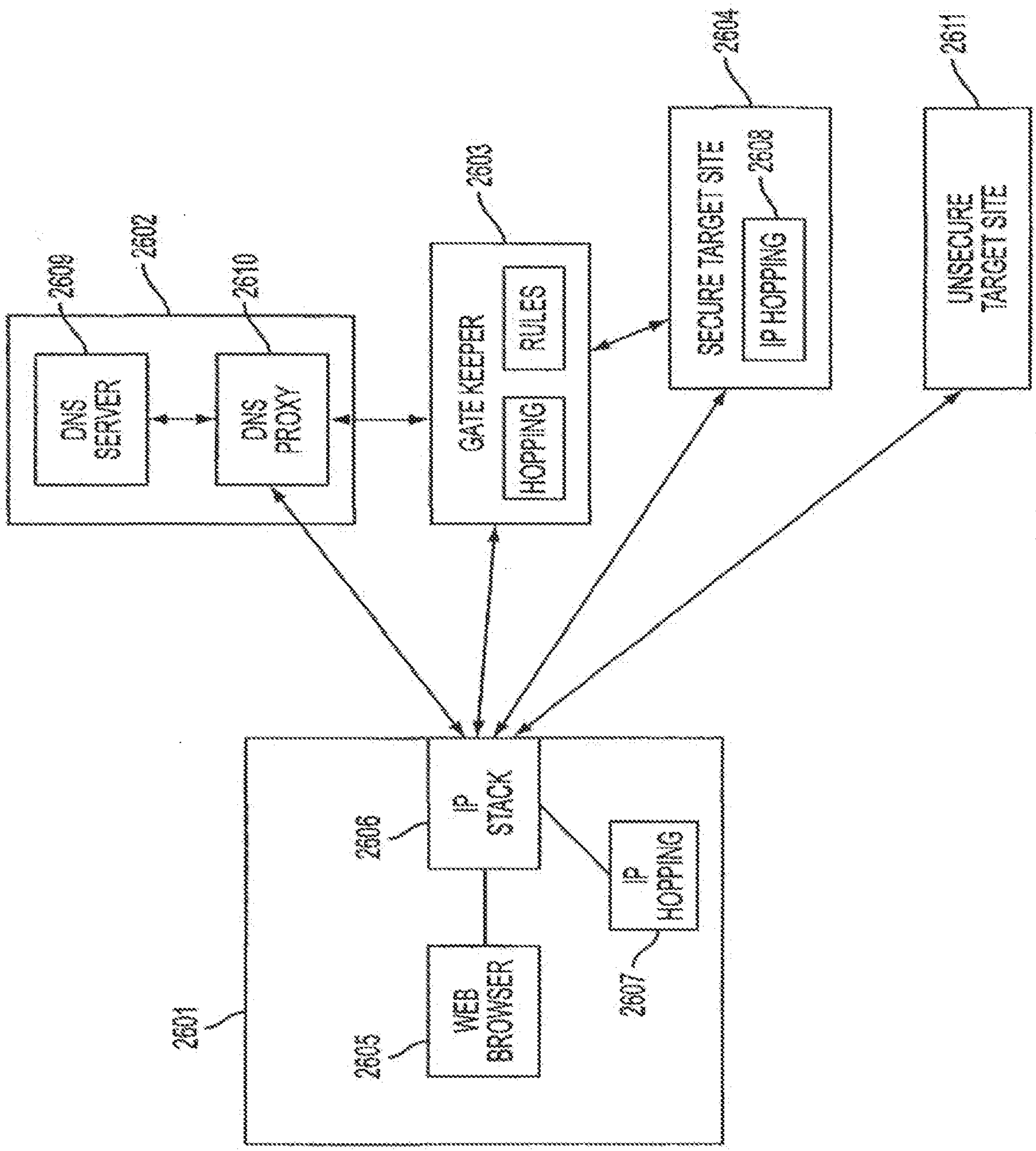

2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
DNS SERVER
DNS PROXY
GATE KEEPER
HOPPING
RULES
SECURE TARGET SITE
IP HOPPING
UNSECURE TARGET SITE
WEB BROWSER
IP STACK
IP HOPPING

FIG. 26

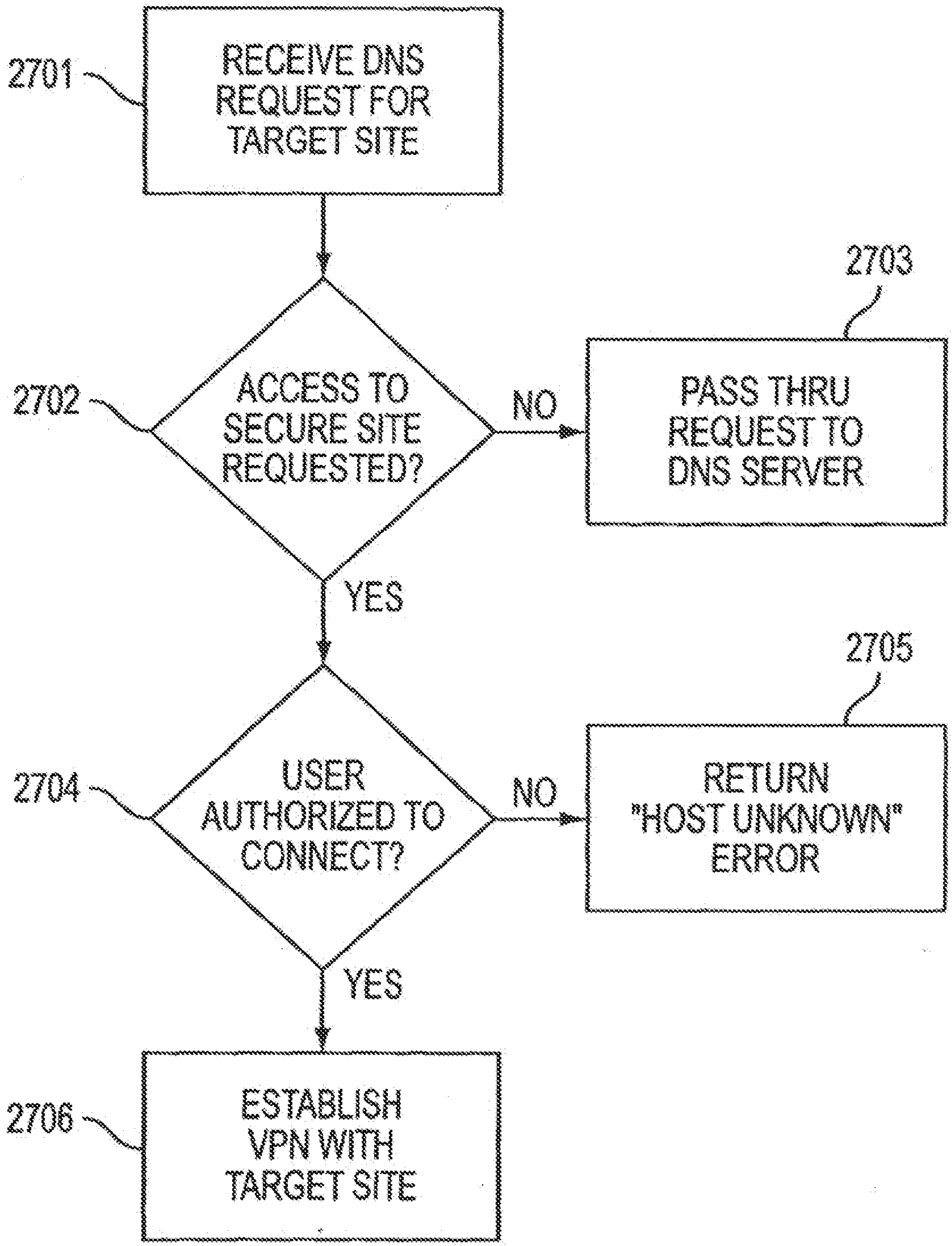

2701
RECEIVE DNS REQUEST FOR TARGET SITE
2702
ACCESS TO SECURE SITE REQUESTED?
NO
2703
PASS THRU REQUEST TO DNS SERVER
YES
2704
USER AUTHORIZED TO CONNECT?
NO
2705
RETURN "HOST UNKNOWN" ERROR
YES
2706
ESTABLISH VPN WITH TARGET SITE

FIG. 27

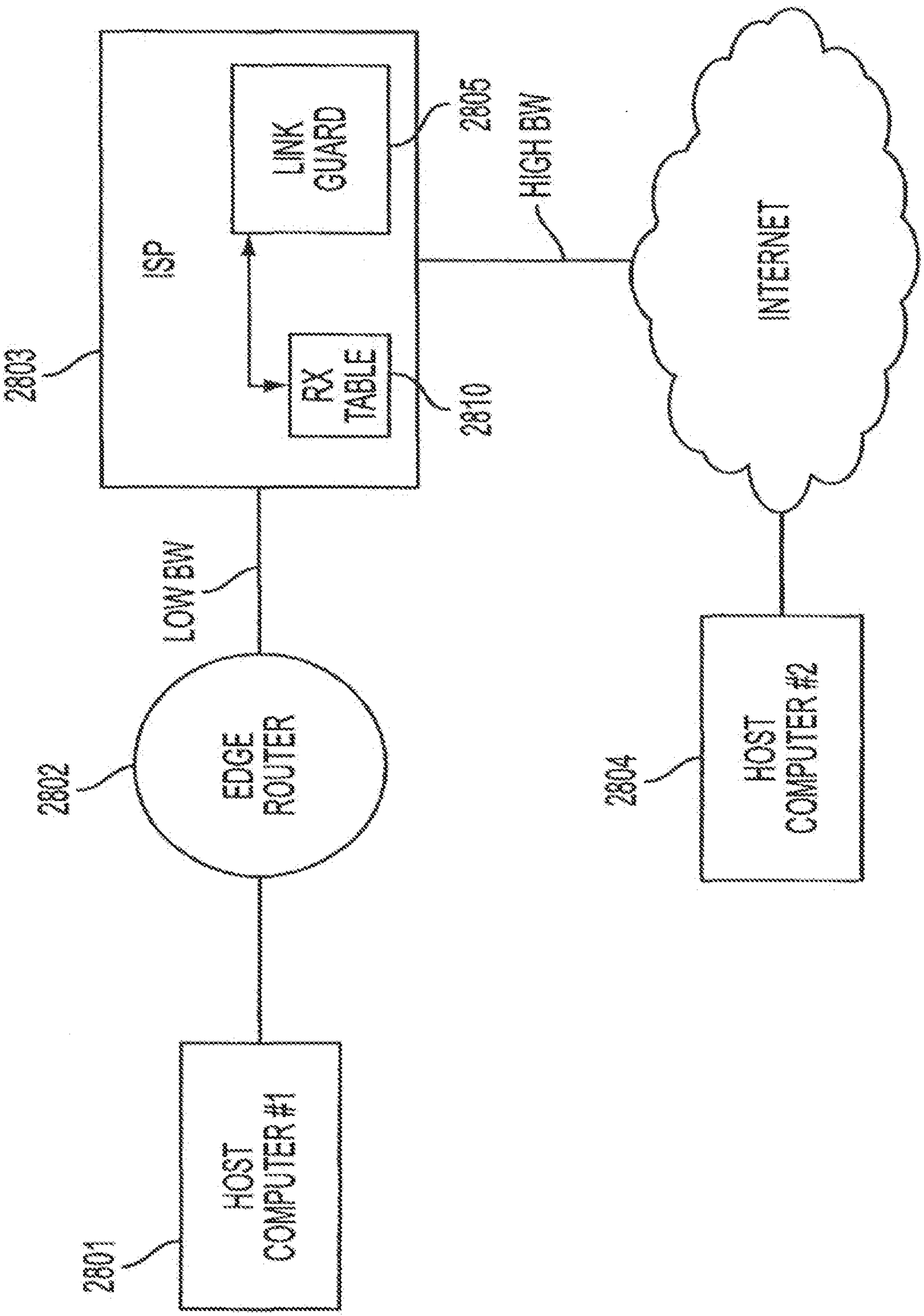

HOST
COMPUTER #1
2801
EDGE
ROUTER
2802
LOW BW
ISP
2803
RX
TABLE
2810
LINK
GUARD
2805
HIGH BW
INTERNET
HOST
COMPUTER #2
2804

FIG. 28

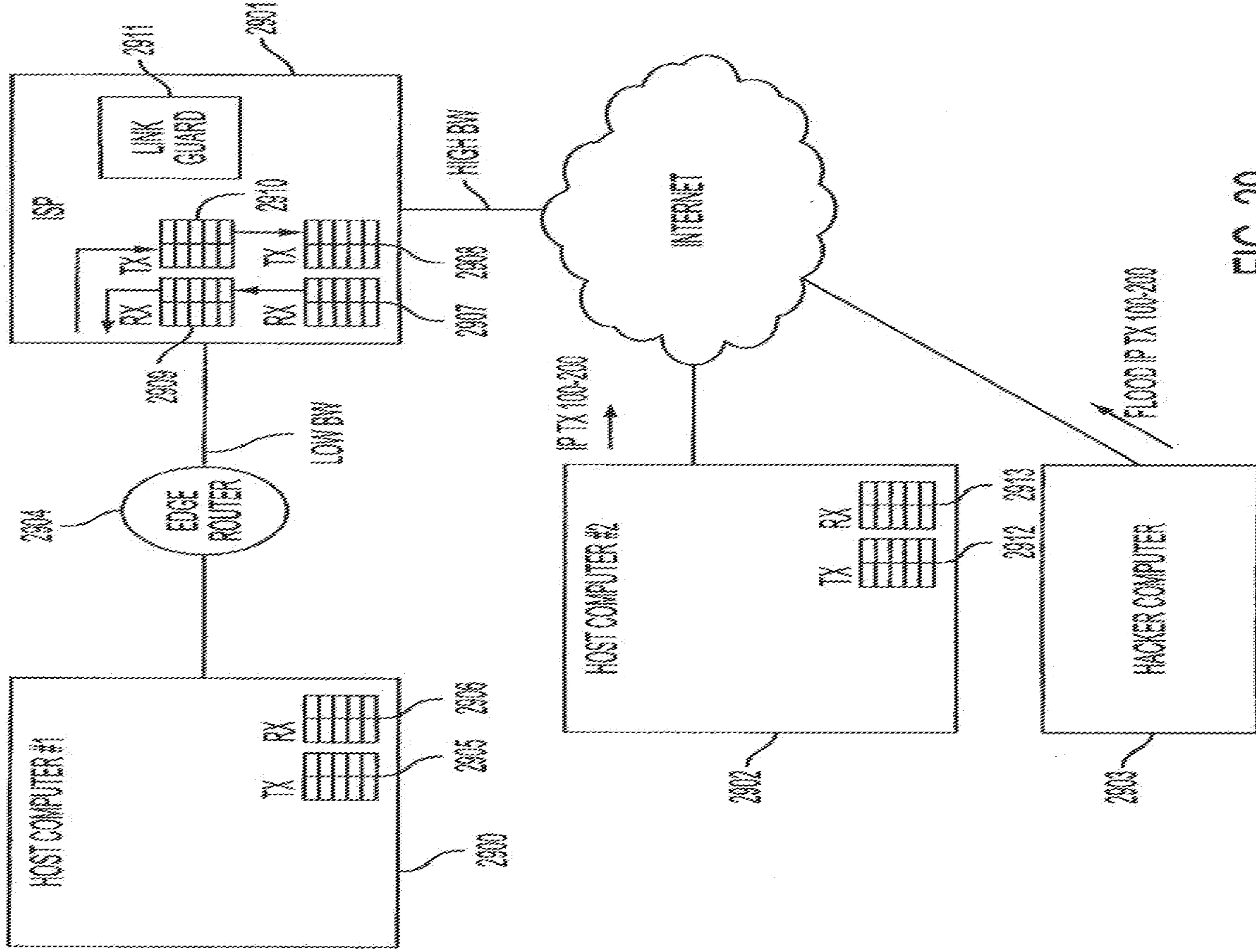

HOST COMPUTER #1
TX
RX
2900
2905
2906
EDGE ROUTER
2304
LOW BW
ISP
RX
TX
RX
TX
LINK GUARD
2909
2910
2911
2901
2907
2908
HIGH BW
INTERNET
IP TX 100-200
HOST COMPUTER #2
TX
RX
2902
2912
2913
HACKER COMPUTER
2903
FLOOD IP TX 100-200

FIG. 29

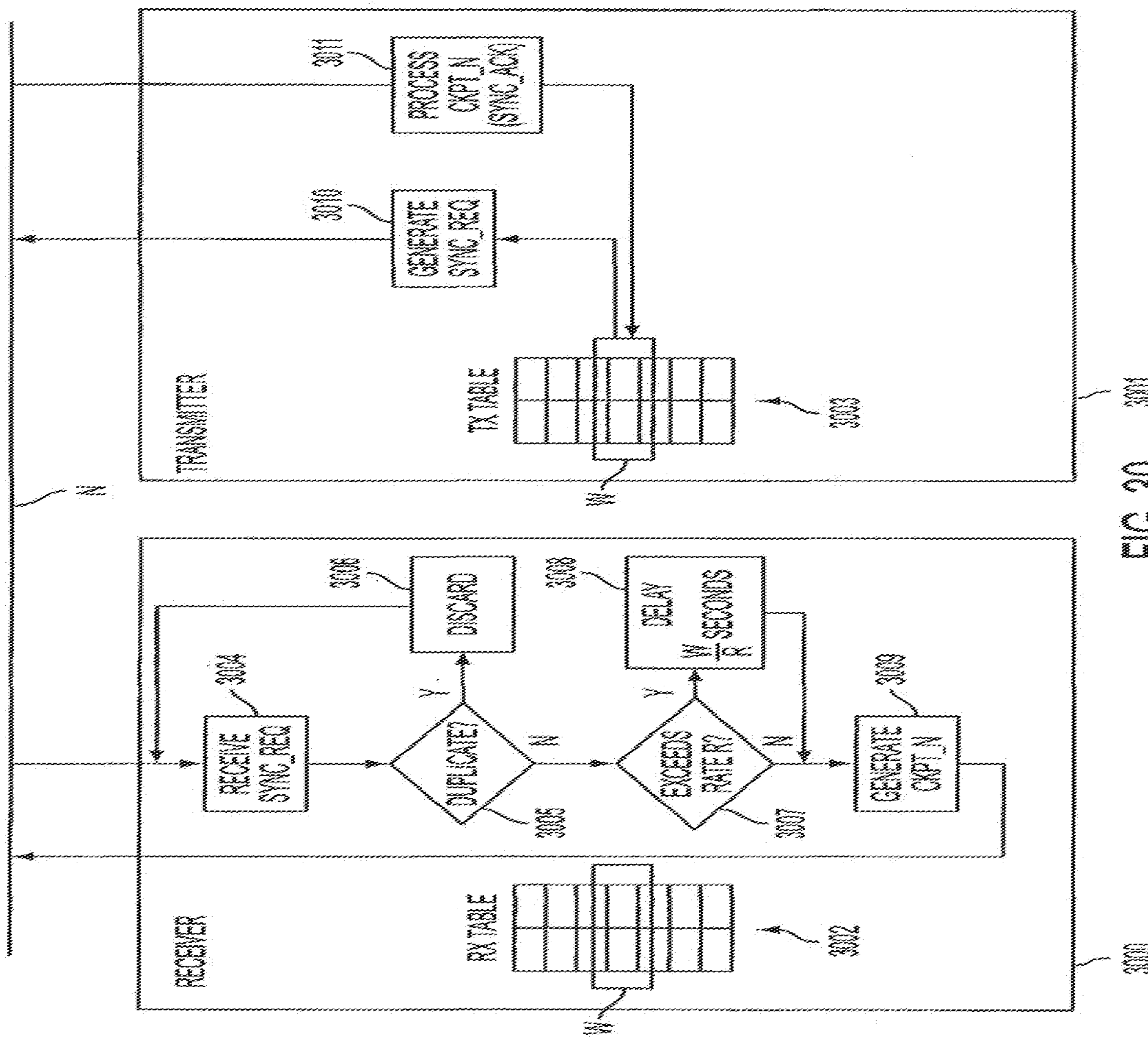

TRANSMITTER
PROCESS CKPT_N (SYNC_ACK)
3011
GENERATE SYNC_REQ
3010
TX TABLE
3003
W
N
RECEIVER
RECEIVE SYNC_REQ
3004
DUPLICATE?
3005
Y
N
DISCARD
3006
EXCEEDS RATE R?
3007
DELAY W/R SECONDS
3008
GENERATE CKPT_N
3009
RX TABLE
3002
3000
3001

FIG. 30

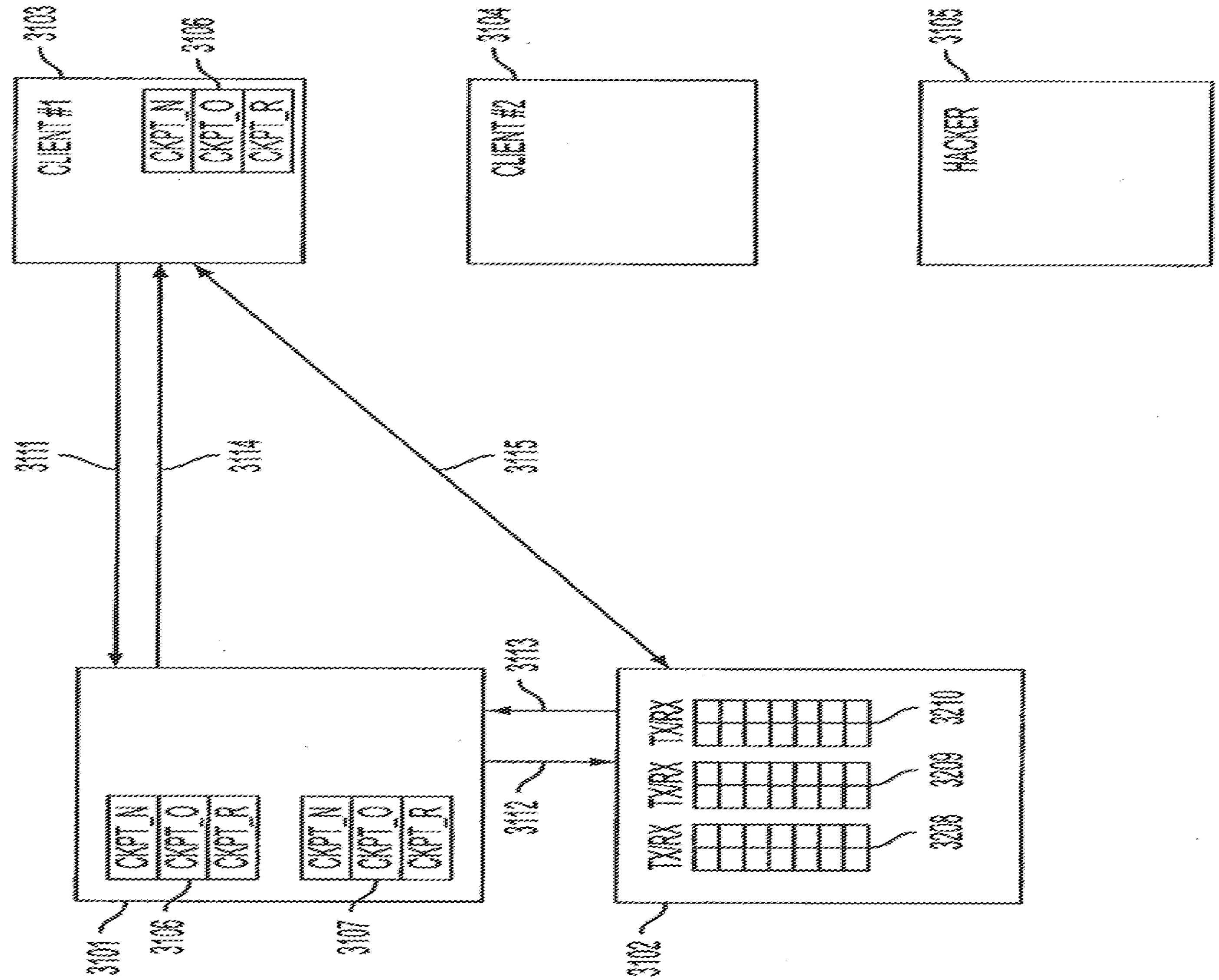

3103
CLIENT #1
3106
CKPT_N
CKPT_O
CKPT_R
3104
CLIENT #2
3105
HACKER
3111
3114
3115
3101
3106
CKPT_N
CKPT_O
CKPT_R
3107
CKPT_N
CKPT_O
CKPT_R
3112
3113
3102
TX/RX
TX/RX
TX/RX
3208
3209
3210

FIG. 31

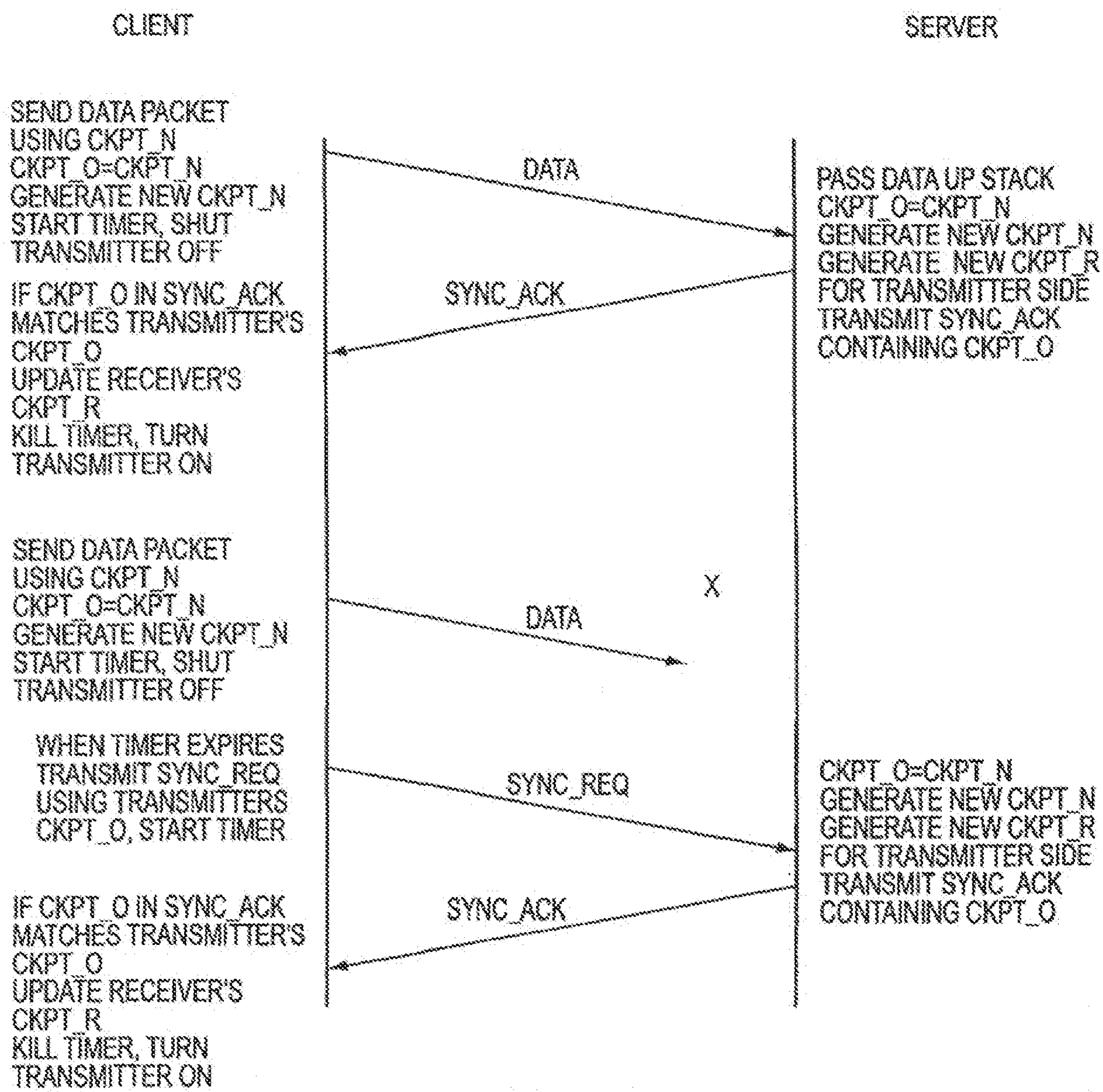

CLIENT
SERVER
SEND DATA PACKET USING CKPT_N CKPT_O=CKPT_N GENERATE NEW CKPT_N START TIMER, SHUT TRANSMITTER OFF
DATA
PASS DATA UP STACK CKPT_O=CKPT_N GENERATE NEW CKPT_N GENERATE NEW CKPT_R FOR TRANSMITTER SIDE TRANSMIT SYNC_ACK CONTAINING CKPT_O
SYNC_ACK
IF CKPT_O IN SYNC_ACK MATCHES TRANSMITTER'S CKPT_O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

FIG. 32

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority from and is a continuation-in-part of previously filed U.S. application Ser. No. 09/429,643, filed on Oct. 29, 1999. The subject matter of that application, which is bodily incorporated herein, derives from provisional U.S. application No. 60/106,261 (filed Oct. 30, 1998) and No. 60/137,704 (filed Jun. 7, 1999).

BACKGROUND OF THE INVENTION

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

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

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

To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple

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

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

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

Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile

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

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

Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet **140** undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called agile routing. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

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

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

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

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

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

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

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

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

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

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

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

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FIG. 20 shows a system employing distributed transmission paths.

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

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

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

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

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

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

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

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

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

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

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

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

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

DETAILED DESCRIPTION OF THE INVENTION

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

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

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

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

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

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

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

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

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

1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence.
2. An interleave sequence number—an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.
3. A time-to-live (TTL) datum—indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.
4. Data type identifier—indicates whether the payload contains, for example, TCP or UDP data.
5. Sender's address—indicates the sender's address in the TARP network.
6. Destination address—indicates the destination terminal's address in the TARP network.
7. Decoy/Real—an indicator of whether the packet contains real message data or dummy decoy data or a combination.

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

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

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

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

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

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. 4, a TARP transceiver 405 can be an originating terminal 100, a destination terminal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

S10. The TARP packet is encrypted using the memorized link key.

S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. SCALABILITY ENHANCEMENTS

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

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

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

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

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

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

When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

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

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

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

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

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

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

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

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

2. FURTHER EXTENSIONS

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

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

A. Hardware Address Hopping

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FIG. 12B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node.

Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

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

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

B. Extending the Address Space

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

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

C. Synchronization Techniques

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

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

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

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

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

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

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

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

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

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

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

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

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

D. Other Synchronization Schemes

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

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

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

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

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

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

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

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

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

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

E. Random Number Generator with a Jump-Ahead Capability

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

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

$$X_i=(aX_{i-1}+b) \bmod c, \tag{1}$$

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

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

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

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

It can be shown that:

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

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

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

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

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

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

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

F. Random Number Generator Example

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

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

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

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

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

TABLE 1

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

G. Fast Packet Filter

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

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

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

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

H. Presence Vector Algorithm

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

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

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

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

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

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

I. Further Synchronization Enhancements

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

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

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

1. There is no need for an efficient jump ahead in the random number generator,
2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
3. No timer based re-synchronization is necessary. This is a consequence of 2.
4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

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

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

3. CONTINUATION-IN-PART IMPROVEMENTS

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

A. Load Balancer

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Suppose that a first link L1 can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L2 can sustain 75 Mb/s and has a window size of 24; and link L3 can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200 Mb/s. The steady state traffic weights are 0.5 for link L1; 0.375 for link L2, and 0.125 for link L3. MIN=1 Mb/s, THRESH=0.8 MESS_T for each link, α=0.75 and β=0.5. These traffic weights will remain stable until a link stops for synchronization or reports a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link L1 receives a SYNC_ACK containing a MESS_R of 24, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link 1 would be below THRESH (0.8). Consequently, link L1's traffic weight value would be reduced to 0.12825, while link L2's traffic weight value would be increased to 0.65812 and link L3's traffic weight value would be increased to 0.217938.
2. Link L2 and L3 remained healthy and link L1 stopped to synchronize. Then link L1's traffic weight value would be set to 0, link L2's traffic weight value would be set to 0.75, and link L33's traffic weight value would be set to 0.25.
3. Link L1 finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be below THRESH. Link L1's traffic weight value would be increased to 0.005, link L2's traffic weight value would be decreased to 0.74625, and link L3's traffic weight value would be decreased to 0.24875.
4. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T

(32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.2525, while link L2's traffic weight value would be decreased to 0.560625 and link L3's traffic weight value would be decreased to 0.186875.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Large Link to Small Link Bandwidth Management

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

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

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

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

In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc 2401], the packets have IP protocols 420 and 421. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, 2805, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid.

According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP 2903 maintains a copy 2910 of the receive table used by host computer 2901. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard 2805 validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc 2104].

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

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

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

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

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

D. Traffic Limiter

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

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

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

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

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

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

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

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

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

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

In accordance with the improvements described above, receiving computer 3000 performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. 30. In step 3004, receiving computer 3000 receives the SYNC_REQ message. In step 3005, a check is made to determine whether the request is a duplicate. If so, it is discarded in step 3006. In step 3007, a check is made to determine whether the SYNC_REQ received from transmitter 3001 was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step 3008 the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

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

E. Signaling Synchronizer

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

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

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

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

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

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

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

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

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

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

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

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

1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer T1 noting CKPT_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.
2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and and other information (i.e user credentials) contained in the inner header. It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT R and transmits a SYNC ACK containing CKPT_O in its payload.
3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.
4. T1 expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPT_O associated with the timer, it starts timer T1 noting CKPT_O again, and a SYNC_REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.
5. When the server receives a SYNC_REQ on its CKPT_N it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.
6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

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

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

CKPT_N. it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

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

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

What is claimed is:

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

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

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

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

2. The method of claim 1, wherein steps (2) and (3) are performed at a DNS server separate from the client computer.

3. The method of claim 1, further comprising the step of:

(4) in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and returning the IP address to the client computer.

4. The method of claim 1, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request.

5. The method of claim 1, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request.

6. The method of claim 1, wherein step (3) comprises the step of establishing the VPN by creating an IP address hopping scheme between the client computer and the target computer.

7. The method of claim 1, wherein step (3) comprises the step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer.

8. The method of claim 1, wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site.

9. The method of claim 5, wherein step (3) comprises the step of transmitting a message to the client computer to determine whether the client computer is authorized to establish the VPN target computer.

10. A system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer, comprising:

a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested; and

a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server.

11. The system of claim 10, wherein the gatekeeper computer creates the VPN by establishing an IP address hopping regime that is used to pseudorandomly change IP addresses in packets transmitted between the client computer and the secure target computer.

12. The system of claim 10, wherein the gatekeeper computer determines whether the client computer has sufficient security privileges to create the VPN and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN.

13. A method of establishing communication between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers, the method comprising the steps of:

(1) in the central computer, receiving from one of the plurality of client computers a request to establish a connection;

(2) authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client;

(3) responsive to a determination that the request is from an authorized client, allocating resources to establish a virtual private link between the client and a second computer; and

(4) communicating between the authorized client and the second computer using the virtual private link.

14. The method of claim 13, wherein step (4) comprises the step of communicating according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence.

15. The method of claim 14, wherein step (4) comprises the step of comparing an Internet Protocol (IP) address in a header of each data packet to a table of valid IP addresses maintained in a table in the second computer.

16. The method of claim 15, wherein step (4) comprises the step of comparing the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window.

17. The method of claim 13, wherein step (2) comprises the step of using a checkpoint data structure that maintains synchronization of a periodically changing parameter known by the central computer and the client computer to authenticate the client.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,502,135 B1 Page 1 of 1
DATED : December 31, 2002
INVENTOR(S) : Edmund Colby Munger et al.

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

Title page,
Item [56], **References Cited**, OTHER PUBLICATIONS, insert the following:

-- Search Report (dated 8/20/02), International Application No. PCT/US01/04340
Search Report (dated 8/23/02), International Application No. PCT/US01/13260
James E. Bellaire, "New Statement of Rules -- Naming Internet Domains", Internet Newsgroup, July 30, 1995, 1 page.
D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, August 1, 1998, pages 22-25.
August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, Vol. 17, No. 4, 1998, pages 293-298.
Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, June 21, 1997, 4 pages. --

Column 48,
Line 2, "VPN target computer" has been replaced with -- VPN with the target computer --.

Signed and Sealed this

Ninth Day of September, 2003

JAMES E. ROGAN
Director of the United States Patent and Trademark Office

PTO-1683
(Rev. 7-96)

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A166	5,007,051	04/09/1991	Dolkas et al.	

U.S. PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes - Number 4 - Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
						Yes	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/virnetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1258	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001789 pp. 1-18, dated December 20, 2012	
	D1259	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001851 pp. 1-13, dated December 30, 2012	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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	
	D1288	iPod Touch Features Guide, 98 pages, 2008	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1339	VirnetX Contact Information, 4 pages, 2011	
	D1340	VirnetX Launches Secure Domain Name Initiative; 4G/LTE Security, 1 page, 2010	
	D1341	VirnetX Gabriel Connection; Enabling Safe Network Neighborhoods, 2 pages, 2012	
	D1342	Baugher et al., "The Secure Real-Time Transport Protocol (SRTP)," Network Working Group, RFC:3711, 39 pages, 2004	
	D1343	Jennings et al., "Resource Location and Discovery (Reload) Draft-Bryan-P2PSIP-Reload-04," Internet-Draft, 12/12/08, pages 1-127	
	D1344	Barnes et al., "Verification Involving PSTN Reachability: Requirements and Architecture Overview," Internet Draft, 27 pages, 2012	
	D1345	April Inc. Form 10-K (Annual Report) filed 12/01/05 for the Period Ending 09/24/05, Edgar Online, 1400 pages, 2011	
	D1346	Phone, Facetime; "Be in Two Places at Once," 3 pages, Printed from the Website http://www.apple.com/ios/facetime/	
	D1347	Apple Press Info; Apple Presents iPhone 4, All-New Design with FaceTime Video Calling, Retina, Display, 5 Megapixel Camera & HD Video Recording, 3 pages, 2010	
	D1348	NYSE AMEX:VHC; Cowen and Co. 39th Annual Technology Media & Telecom Conference, 36 pages, June 2, 2011	
	D1349	Pindyck et al., "Market Power: Monopoly and Monopsony," Microeconomics, Sixth Edition, pages 370-371	
	D1350	Press Release; IpCapital Group Completes VirnetX IP Licensing Evaluation, 3 pages	
	D1351	Microsoft Real-Time Communications: Protocols and Technologies, Microsoft TechNet, 22 pages, 2010	
	D1352	Filing Receipt dated September 23, 2011 for Application Number: 13/223,259	
	D1353	Email Communications Regarding Apple Product Innovations, 6 pages, 2010	
	D1354	Mathy et al., "Traversal Using Relays Around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," Internet Engineering Task Force (IETF), RFC: 5766, 67 pages, 2010	
	D1355	Egevang et al., "The IP Network Address Translator (NAT)," Network Working Group, RFC: 1631, 10 pages, 1994	
	D1356	Srisuresh et al., "IP Network Address Translator (NAT) Terminology and Considerations," Network Working Group, RFC:2663, 30 pages, 1999	
	D1357	Sisalem, et al., "Introduction to Cryptographic Mechanisms," SIP Security, 356 pages, 2009	
	D1358	Curriculum Vitae, Mark T Jones, 9 pages	
	D1359	Curriculum Vitae, Roy Weinstein, 5 pages	
	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/virnetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1362	iPhone, FaceTime; "Be in Two Places at Once," 3 pages, Printed from Website: http://www.apple.com/ios/facetime/	
	D1363	iPhone, "It Does Everything Better,"6 pages, Printed from Website: http://www.apple.com/iPhone/built-in-apps	
	D1364	My Apple ID, "What's an Apple ID," 1 pages, Printed from Website: https://appleid.apple.com/cgi-bin/webobjects/myappleid.woa	
	D1365	Rosenberg et al., "Session Initiation Protocol (SIP): Locating SIP Servers," Network Working Group, RFC: 3263, 17 pages, 2002	
	D1366	Certified Copy dated September 21, 2012 of Reexamination Certificate Number 6,502,135 issued June 6, 2011, 11 pages	
	D1367	Certified Copy dated September 20, 2012 of Patent Application Number 95/001,269, 4999 pages	
	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1385	Binmore, "The Nash Bargaining Solution in Economic Modelling," The Rand Journal of Economics, 17:176-188, 1996	
	D1386	Rubinstein et al., "On the Interpretation of the Nash Bargaining Solution and its Extension to Non-Expected Utility Preferences," Econometrica, 60:1171-1186, 1992	
	D1387	Greenleaf et al., "Guarantees in Auctions: The Auction House as Negotiator and Managerial Decision Maker," Management Science, 39:1130-1145, 1993	
	D1388	Chan, "Trade Negotiations in a Nash Bargaining Model," Journal of International Economics, 25:253-363, 1987	
	D1389	Lemley et al., "Patent Holdup and Royalty Stacking," Texas Law Review, 85:1991-2049	
	D1390	Cauley, "Winning the Patent Damages Case; A Litigator's Guide to Economic Models and Other Damage Strategies," Oxford Press, pages 29-30, 2044	
	D1391	Degnan et al., "A Survey of Licensed Royalties," Les Nouvelles, pages 91, 93, 94, 1997	
	D1392	Kahn, "The Review of Economics and Statistics," pages 157-164, 1993	
	D1393	Microsoft Company Information; Including Stocks and Financial Information, 83 pages	
	D1394	Apple Press Info: Apple Updates MacBook Pro with Next Generation Processors, Graphics & Thunderbolt I/O Technology, 3 pages, Printed from Website: http://www.apple.com/pr/library/2011/02/24Apple-Updates-MacBook-Pro-with-Next-Generation-Processors-Graphics-Thunderbolt-I-O-Technology.html	
	D1395	Apple Press Info: Apple to Ship Mac OS X Snow Leopard on August 28, 2 pages, Printed from the Website: http://www.apple.com/pr/library/2009/08/24/apple-to-ship-mac-os-x	
	D1396	iPad, Facetime; "Once Again, iPad gets the World Talking," 3 pages, Printed from the Website: http://www.apple.com/ipad/built-in-apps/facetime/html	
	D1397	Apple iOS: Setting up VPN, 2 pages, Printed from Website: http/support.apple.com/kb/HT1424	
	D1398	Apple iPhone User Guide for iOS 5.1 Software, 179 pages, 2012	
	D1399	Apple, Communicating with HTTP Servers, CFNetworking Programming Guide, 6 pages, 2011, Printed from the Website: https://developer.apple.com/library/ios/documentation/networking/conceptual/CFNetwork/CFHT	
	D1400	VirnetX, Gabriel Connection Technology ™ White Paper, 7 pages, 2012	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	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)	
	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	

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	**13/336,790**
				Filing Date	**12-23-2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Krisna Lim**
				Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

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

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

[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 A166 from Canadian office action dated December 27, 2012; Cited reference C25 from Japanese office action dated 12/13/12; Cited references C26-28; D1254, 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.

[ ] 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: February 15, 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 41026995-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	14977672
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-FEB-2013
Filing Date:	23-DEC-2011
Time Stamp:	20:56:39
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	D1368.pdf	4010571 66eda3aa87b351f7a3dcf665f7a5bb668bcf6b56	no	18

Warnings:

Information:

2	Non Patent Literature	D1369.pdf	2056403 b2a95f7d98d3f163cb905c472f12762148e96fa8	no	8
Warnings:					
Information:					
3	Non Patent Literature	D1370.pdf	2578314 e2cf986767b9aa357b16bab04ab84b7900f5ba01	no	14
Warnings:					
Information:					
4	Non Patent Literature	D1371.pdf	2505462 7bb5878fb0e7ec7d03176d54f5b8f18e07c30e26	no	13
Warnings:					
Information:					
5	Non Patent Literature	D1372.pdf	1853041 757e5268612a855ffbefbecbe0e552195f952390	no	4
Warnings:					
Information:					
6	Non Patent Literature	D1373.pdf	2537596 dc0ad5cf25dbb7187b146f0cc63ca4fb5f2fb06f	no	8
Warnings:					
Information:					
7	Non Patent Literature	D1374.pdf	1977415 1ce1f630928a50231badb85c908b788d6755966a	no	4
Warnings:					
Information:					
8	Non Patent Literature	D1375.pdf	3710663 917cb9a7b3bdfea3ef674d221533f4bda978fb3d	no	27
Warnings:					
Information:					
9	Non Patent Literature	D1376.pdf	143571 fad0e8e3f3b9c45b319d5abae8e2ae4121d989ec	no	2
Warnings:					
Information:					
10	Non Patent Literature	D1379.pdf	777157 afe6e775d93ba3d86e5a5bff0fd6f203f7b41fa5	no	5
Warnings:					
Information:					

11	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:					
12	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:					
13	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:					
14	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:					
15	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:					
16	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:					
17	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:

18	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:

19	Non Patent Literature	D1377.pdf	169639 49df2a0869659c98b13aa37fb5cf678872bd1b75	no	19

Warnings:

Information:

20	Non Patent Literature	D1378.pdf	64023 41ca085d82ea2b7696453c8044626b59802a23d1	no	6

Warnings:

Information:

21	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:

22	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:

23	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:

24	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:

25	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:

26	Non Patent Literature	D1393.pdf	9736160 690ab3b8b45484a583e03e513fd8dfabf58fbc25	no	83

Warnings:

Information:

27	Non Patent Literature	D1398part2.pdf	2722312 4b0cbff58fdd586cd698fc3f20a45f337e52bd97	no	30

Warnings:

Information:

28	Non Patent Literature	D1401.pdf	253888 ce6544195e609f1f578a1f6c5e0a8a0b80cc2eee	no	4

Warnings:

Information:

29	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:

30	Non Patent Literature	D1405.pdf	116396 eaeec236192eecc32d9cf306d2563942aa375926	no	2

Warnings:

Information:

31	Non Patent Literature	D1406.pdf	1483724 8f4bd461e0b2df6b3aa6ba4cfcdeff73b15daaa5	no	18

Warnings:

Information:

32	Non Patent Literature	D1394.pdf	97596 970ea389448b4dc0ae7efc8562e425f182c86889	no	3

Warnings:					
Information:					
33	Non Patent Literature	D1395.pdf	337068 f616b207e367d403339d7bce73e91992588 7ccca	no	2
Warnings:					
Information:					
34	Non Patent Literature	D1396.pdf	658944 441e7c81e2ca02615462fd3c26a0159a01fe ec75	no	3
Warnings:					
Information:					
35	Non Patent Literature	D1397.pdf	60279 358af2f1b62d3f83c602d5f407fa093ec5293 7f3	no	2
Warnings:					
Information:					
36	Non Patent Literature	D1399.pdf	333444 1ae45dff83698332784578247 5b139131dd d6853	no	6
Warnings:					
Information:					
37	Non Patent Literature	D1403.pdf	5321642 30c73b64ca748696c3217bc2c0eab3496f5 8d686	no	10
Warnings:					
Information:					
38	Non Patent Literature	D1402.pdf	14706584 eda4a90563431f193cf89771b831b0277da 24f3f	no	64
Warnings:					
Information:					
39	Non Patent Literature	D1398part3.pdf	3983385 fa265306ed581ab3c273df3c8140634112d 1cfdb	no	89
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
40	Non Patent Literature	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:					
41	Non Patent Literature	D1400.pdf	285807 d2efb93ba54c5467fcaf4801bdd81ce569b8aca4	no	7
Warnings:					
Information:					
42	Non Patent Literature	D1398part1.pdf	1890669 2c3253e124a848b7a0cc09ee1050145dfc09bb8a	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:					
43	Non Patent Literature	D1408.pdf	1969680 c4e9f131b17b976f7512f0a8ff5ec0413c08f460	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:					
44	Non Patent Literature	D1409.pdf	184126 748e7c68d71553217eaa4ba6ee615a582558c95c	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:					
45	Non Patent Literature	D1410.pdf	240704 9b1e5bc837ef6cd09ee58bcc4ef16be5d62f249d	no	3
Warnings:					
Information:					
46	Non Patent Literature	D1411.pdf	1246690 8f56d4c2bbb422c0696dd9a42c8390b8331169d5	no	12
Warnings:					
Information:					
47	Non Patent Literature	IDS.pdf	82398 f37a66d0c47e19355bbedae32535671106ed9ff8	no	9
Warnings:					
Information:					
			Total Files Size (in bytes):	92121788	

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:	14977382
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-FEB-2013
Filing Date:	23-DEC-2011
Time Stamp:	20:57:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1367part60.pdf	6773524 7d88e8851457b6ec52c0e506743776308e8cfab3	no	200

Warnings:

Information:

2	Non Patent Literature	D1367part61.pdf	6755777 d86235569ce34aab55a7ba3b1cfb3eeedbc5d895	no	200
Warnings:					
Information:					
3	Non Patent Literature	D1367part62.pdf	6058621 fdb98d4cd4a610bc5206ddea9b870c9c2f63b03d	no	200
Warnings:					
Information:					
4	Non Patent Literature	D1367part63.pdf	5968372 58c23cf102e013185469ea1768e1fb40df7c07c3	no	200
Warnings:					
Information:					
5	Non Patent Literature	D1367part64.pdf	5493823 76fa05ded24ff89bf3dc542c2a8e062ff32eb19a	no	200
Warnings:					
Information:					
6	Non Patent Literature	D1367part65.pdf	8929581 498f89623b235dfff910de52c69e435a4339a8ce	no	200
Warnings:					
Information:					
7	Non Patent Literature	D1367part66.pdf	8355250 e70796817e7f1ace3a8bd94ad48f83e06ad3571f	no	200
Warnings:					
Information:					
8	Non Patent Literature	D1367part67.pdf	6039483 313887801f0db75273c9f17ebcbb4857770ad0fa	no	200
Warnings:					
Information:					
9	Non Patent Literature	D1367part68.pdf	4701060 76c54663b19e4cdc6de528e1d02526310d99f594	no	200
Warnings:					
Information:					
10	Non Patent Literature	D1367part69.pdf	5677709 bf9092148071fa016dd283e4653d16387d207e3f	no	200
Warnings:					
Information:					

11	Non Patent Literature	D1367part70.pdf	5346438 b0bdb5bf643c66a6c547b118acbde76e5c2fafd1	no	200
Warnings:					
Information:					
12	Non Patent Literature	D1367part71.pdf	6946216 83161ad44c5a2afabed818c4c84a7478dd13ccbf	no	200
Warnings:					
Information:					
13	Non Patent Literature	D1367part72.pdf	5859323 d34bd2e2f0b1d4c250f9f1e66208227fed296bae	no	200
Warnings:					
Information:					
14	Non Patent Literature	D1367part73.pdf	6310488 acaa235876d1179a8cab197e868278103e8a6974	no	200
Warnings:					
Information:					
15	Non Patent Literature	D1367part74.pdf	9839138 5fa9f7bce783d1983da23c8f76aa161503d47140	no	200
Warnings:					
Information:					
16	Non Patent Literature	D1367part75.pdf	11273482 d1aabce64442d1b48834bedcdf8f4fb1cf195d91	no	199
Warnings:					
Information:					
17	Non Patent Literature	D1367part76.pdf	7216090 93fbd52354a7f9e43d0870b497cd80fe70513685	no	200
Warnings:					
Information:					
18	Non Patent Literature	D1367part77.pdf	5080937 c9aeb857311e82f677054681a14dc773defd5d3b	no	200
Warnings:					
Information:					
19	Non Patent Literature	D1367part78.pdf	5274671 708cbdfc075dbd09ceaf5511b91b095fdd6e9965	no	200
Warnings:					
Information:					

20	Non Patent Literature	D1367part79.pdf	6569921 1da47975c80f84d11cd8d8b097d5a432497bc43f	no	200
Warnings:					
Information:					
21	Non Patent Literature	D1367part80.pdf	6689283 045a83d2772c7dd35809ceecb9ba8b3d2f91c07f	no	200
Warnings:					
Information:					
22	Non Patent Literature	D1367part81.pdf	5447539 1f3b5c89c31c23e3c21668dccb615fe9fe5ab0c0	no	200
Warnings:					
Information:					
23	Non Patent Literature	D1367part82.pdf	5454275 42f253321fcb946f15f6b06c94adcc3cb6260af1	no	200
Warnings:					
Information:					
24	Non Patent Literature	D1367part83.pdf	5512481 49daf8c3370f73515395920b6aff5af913c7917e	no	200
Warnings:					
Information:					
25	Non Patent Literature	D1367part84.pdf	5319561 8b24b3553d256da42e4b44cb07b2366141720aad	no	200
Warnings:					
Information:					
26	Non Patent Literature	D1367part85.pdf	5516946 05541fe9c7bafcf80862e078892d159b7188cacb	no	200
Warnings:					
Information:					
27	Non Patent Literature	D1367part86.pdf	5082603 78d8c0955c953525921230119d98416974793bf6	no	200
Warnings:					
Information:					
28	Non Patent Literature	D1367part87.pdf	6006794 f2197a942a8d43c4923a1b839421fc2fa7c4fbe4	no	200
Warnings:					
Information:					

29	Non Patent Literature	D1367part88.pdf	5043145 fa379b985035db02f7bf256f674829d66ea9c0a7	no	200
Warnings:					
Information:					
30	Non Patent Literature	D1367part89.pdf	6423612 aa882a989be9579974a5b9e930d874de4c85d17e	no	200
Warnings:					
Information:					
31	Non Patent Literature	D1367part90.pdf	5293567 ce4708b0fab68d47c692cf45db1c80f7767377c8	no	200
Warnings:					
Information:					
32	Non Patent Literature	D1367part91.pdf	5481870 87c4160aed537a8949c8405ca44adcaf0cc1fc69	no	200
Warnings:					
Information:					
33	Non Patent Literature	D1367part92.pdf	6369650 5606b56694b6e467a3124540b457b504f73ca9cf	no	200
Warnings:					
Information:					
34	Non Patent Literature	D1367part93.pdf	5909805 fe992b1450fea1da6b9dfa7207a3528a79e68983	no	200
Warnings:					
Information:					
35	Non Patent Literature	D1367part94.pdf	5218581 55e986f3265c15475039bc763c44b88b81d91281	no	200
Warnings:					
Information:					
36	Non Patent Literature	D1367part95.pdf	5309204 43d2e3ac0ea579c1e86eb02fa5e21748511fe7b5	no	200
Warnings:					
Information:					
37	Non Patent Literature	D1367part96.pdf	4692277 98aa51f250cec36e9855e6e23a70889dc3434578	no	200
Warnings:					
Information:					

38	Non Patent Literature	D1367part97.pdf	7427881 1fed39d36144aff06cce17da34dadce3fd015685	no	200
Warnings:					
Information:					
39	Non Patent Literature	D1367part98.pdf	7415097 cf79f150ec86fd6f0d38862fbf8e9a40ceb232cc	no	200
Warnings:					
Information:					
40	Non Patent Literature	D1367part99.pdf	4328217 17f6384afc549ac0a878e8b75430c58f7f3cd37d	no	200
Warnings:					
Information:					
41	Non Patent Literature	D1367part100.pdf	4450138 c0d855ae089541f5881c67a6324f490fbb2480c9	no	199
Warnings:					
Information:					
42	Non Patent Literature	D1367part101.pdf	7633741 dc3e7dbd30eea1d827f50181fd92e720a1243a52	no	200
Warnings:					
Information:					
43	Non Patent Literature	D1367part102.pdf	6239272 f8fcd4c1fca498541612e72df5cd95020d36c422	no	200
Warnings:					
Information:					
44	Non Patent Literature	D1367part103.pdf	6118485 d537b6bb3743838d991f3fa71a06999990b02295	no	200
Warnings:					
Information:					
45	Non Patent Literature	D1367part104.pdf	6305558 bc39907953cc9bfa6be1c76a38c58074f4129727	no	200
Warnings:					
Information:					
46	Non Patent Literature	D1367part105.pdf	6786238 d4ec58e22c6607f6a4435c4672b798af7022f505	no	200
Warnings:					
Information:					

47	Non Patent Literature	D1367part106.pdf	1857024 9759b7200ae7107d5e26c04d5a98eefb259da112	no	52

Warnings:

Information:

Total Files Size (in bytes):	287802748

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:	14977169
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-FEB-2013
Filing Date:	23-DEC-2011
Time Stamp:	20:58:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1367part1.pdf	15960835 fe4eac6ef853165892de444e6b46f9c8b294 1991	no	201

Warnings:

Information:

2	Non Patent Literature	D1367part2.pdf	3171465 d41604ab63c8e5aaac499ffead29d43cbeb1f4ae	no	200
Warnings:					
Information:					
3	Non Patent Literature	D1367part3.pdf	3067154 eb4e223c50a6efb9b76ad963ca690fc0e148a696	no	200
Warnings:					
Information:					
4	Non Patent Literature	D1367part4.pdf	2754394 27542e3bfcef4163e8eaf027c3f59b3522719945	no	200
Warnings:					
Information:					
5	Non Patent Literature	D1367part5.pdf	3204769 b84f42ec4c8b3735e9e1d10456b0a4239b698cf5	no	200
Warnings:					
Information:					
6	Non Patent Literature	D1367part6.pdf	3562036 b5ea9c4993f34b249ce1de35548d1a328853a064	no	200
Warnings:					
Information:					
7	Non Patent Literature	D1367part7.pdf	3193057 2f0b7e75e2d4676116207937450bd355799f6882	no	200
Warnings:					
Information:					
8	Non Patent Literature	D1367part8.pdf	1736291 5c12f84a88ac4f0b839ca6d18800ccaa2ed770b3	no	200
Warnings:					
Information:					
9	Non Patent Literature	D1367part9.pdf	2778626 997661c418a9b95eb9fd80feb03c6537e59b2ea2	no	200
Warnings:					
Information:					
10	Non Patent Literature	D1367part10.pdf	2220634 136cee2ab62a09694855b9e5026450a12dc45ebf	no	200
Warnings:					
Information:					

11	Non Patent Literature	D1367part11.pdf	2896543 ccfb4ec5c7678f0697fad134148b0a51ef69ec5c	no	200
Warnings:					
Information:					
12	Non Patent Literature	D1367part12.pdf	3275415 54a76826c8a38b1d8d69ba5ca6b12edb294deee3	no	200
Warnings:					
Information:					
13	Non Patent Literature	D1367part13.pdf	2574446 1540300550e6afb5ffabffd0b1702c7bcc47e835	no	200
Warnings:					
Information:					
14	Non Patent Literature	D1367part14.pdf	2870775 33427066647a8efc1b58131ff552d2d39f6cf66c	no	200
Warnings:					
Information:					
15	Non Patent Literature	D1367part15.pdf	3533177 ce6ef0c77a5b674f2eb7a16d8c0b405f4ea9cf3d	no	200
Warnings:					
Information:					
16	Non Patent Literature	D1367part16.pdf	3786071 9784e33a377b4c0ed3296f46a47d237535a4b80f	no	200
Warnings:					
Information:					
17	Non Patent Literature	D1367part17.pdf	2829552 30217a4cf275dc8b68bc609bf783995807a1689f	no	200
Warnings:					
Information:					
18	Non Patent Literature	D1367part18.pdf	2742291 ca4f5a259b8536daa36b8b9ad409f5a1f1f09a66	no	200
Warnings:					
Information:					
19	Non Patent Literature	D1367part19.pdf	2846638 f69ee9b2ba78513e2b92bd0475d69e6a0fb4abc8	no	200
Warnings:					
Information:					

20	Non Patent Literature	D1367part20.pdf	2598677 de08e1f6b55e257936f24575e7fb5b954f37ee49	no	200
Warnings:					
Information:					
21	Non Patent Literature	D1367part21.pdf	3094007 0e0337954535cbbd5c5f97f2ec0ed5f8b5aa5116	no	200
Warnings:					
Information:					
22	Non Patent Literature	D1367part22.pdf	2473740 bb73365c8ef0c521ea22a11451b039e2c73a2672	no	200
Warnings:					
Information:					
23	Non Patent Literature	D1367part23.pdf	1839430 b40eec3f85e92e6fc9a6665e9f4bbd47672ef115	no	200
Warnings:					
Information:					
24	Non Patent Literature	D1367part24.pdf	2109084 55a0beaf6a686ba1cf800865faf64f519baf0f0b	no	200
Warnings:					
Information:					
25	Non Patent Literature	D1367part25.pdf	2066586 aa9ffa2f6eefa7f5c068f45a8ed0bd414648910a	no	199
Warnings:					
Information:					
26	Non Patent Literature	D1367part26.pdf	7803999 15026aae52ef28e0260fc2f06a4c7aa844abdc29	no	200
Warnings:					
Information:					
27	Non Patent Literature	D1367part27.pdf	6949434 4431b64464736425547db671b1f533059c60ae74	no	200
Warnings:					
Information:					
28	Non Patent Literature	D1367part28.pdf	9420516 99f1bc77d51a1c0e59963be6e8125f62582b2d3b	no	200
Warnings:					
Information:					

29	Non Patent Literature	D1367part29.pdf	8622584 f52e7ff9af96e1be67fa0bf4e415c6edc884d6db	no	200
Warnings:					
Information:					
30	Non Patent Literature	D1367part30.pdf	5691420 aff21f5e3c4226b2942d8ea86909f27b84efeae4	no	200
Warnings:					
Information:					
31	Non Patent Literature	D1367part31.pdf	5147177 79a3fb072f1038c5a54619f42af13855c8d61095	no	200
Warnings:					
Information:					
32	Non Patent Literature	D1367part32.pdf	4989115 ff4eec8f363c85b9e96f09e060f053d2ad486b2a	no	200
Warnings:					
Information:					
33	Non Patent Literature	D1367part33.pdf	5568352 d9e1acef97040cfe5cf0175be4737a18634ccc13	no	200
Warnings:					
Information:					
34	Non Patent Literature	D1367part34.pdf	8490123 3dc07e6085f579298408aa4661548536d76d29a6	no	200
Warnings:					
Information:					
35	Non Patent Literature	D1367part35.pdf	6798116 70e0df0fd8749da37e86e377b2db6d4da47cda6f	no	200
Warnings:					
Information:					
36	Non Patent Literature	D1367part36.pdf	3485165 3eced5d52de48ba1800fe1f8ca4af5138044b82b	no	200
Warnings:					
Information:					
37	Non Patent Literature	D1367part37.pdf	4016005 20e974b5331b980e7d7eb529725eff12e8f04a4f	no	200
Warnings:					
Information:					

38	Non Patent Literature	D1367part38.pdf	3636004 fca83e506ae11779b35e45a8c9cffcfcec7dfca1	no	200
Warnings:					
Information:					
39	Non Patent Literature	D1367part39.pdf	4305786 180e4c71fd02cc5906a2c19341d90b2c86311ce1	no	200
Warnings:					
Information:					
40	Non Patent Literature	D1367part40.pdf	4903541 7f108e007a707311b614e8b6605f08c3ca923ed3	no	200
Warnings:					
Information:					
41	Non Patent Literature	D1367part41.pdf	7138830 72be8053f1ae72eb1cb9bd64705ffa64a059e13a	no	200
Warnings:					
Information:					
42	Non Patent Literature	D1367part42.pdf	9911751 f2070eefb592a0e36d503cc8248a74887ca228b0	no	200
Warnings:					
Information:					
43	Non Patent Literature	D1367part43.pdf	7969144 2f0342bb9b82e4dc238a9f292bce6504fac2fdfa	no	200
Warnings:					
Information:					
44	Non Patent Literature	D1367part44.pdf	9714518 69809f99901efd296a487fec6c8953e1e9fb5dbe	no	200
Warnings:					
Information:					
45	Non Patent Literature	D1367part45.pdf	9464624 0e72b0765bd452396169aed99d9a7db2f50f713a	no	200
Warnings:					
Information:					
46	Non Patent Literature	D1367part46.pdf	8840128 ec4819ce60039eeb925758cc05992220baa447cc	no	200
Warnings:					
Information:					

47	Non Patent Literature	D1367part47.pdf	7390404 20f6a873451180115e534ea00e5c96c9098 9a25b	no	200
Warnings:					
Information:					
48	Non Patent Literature	D1367part48.pdf	5183735 9fe8a56297a63015b48d8fc8f90ea07a06fe0 c6e	no	200
Warnings:					
Information:					
49	Non Patent Literature	D1367part49.pdf	6393126 97f0f2fb7616056656bf05eb3b815ac0ade6 0d84	no	200
Warnings:					
Information:					
50	Non Patent Literature	D1367part50.pdf	6962577 de042b7abfe7a3823a7502a00854afdeb35 de8fb	no	199
Warnings:					
Information:					
51	Non Patent Literature	D1367part51.pdf	6443871 86bdf9113d5cb529d8335a5af2a258fda7ec 218a	no	200
Warnings:					
Information:					
52	Non Patent Literature	D1367part52.pdf	6068436 a0c2088b834a5b132fd59e9003d97da8137 9d02a	no	200
Warnings:					
Information:					
53	Non Patent Literature	D1367part53.pdf	6570870 9600469d0807f84cf8dcb941dbc5f4990610 2a72	no	200
Warnings:					
Information:					
54	Non Patent Literature	D1367part54.pdf	4949670 4da01fa51501b8e45d981619e0d3b0e3e5c 462f7	no	200
Warnings:					
Information:					
55	Non Patent Literature	D1367part55.pdf	4695155 12e5f7564ceabb745e9126103bb9ec7f096 75e79	no	200
Warnings:					
Information:					

56	Non Patent Literature	D1367part56.pdf	4957213 8e4df5a225d7b4bd4f869b2dece14d8e6a2e31bf	no	200
Warnings:					
Information:					
57	Non Patent Literature	D1367part57.pdf	8708817 70e6f68114bea0dcb0ecee736a1bb7dfb121a188	no	200
Warnings:					
Information:					
58	Non Patent Literature	D1367part58.pdf	6779256 ed3b9e77755c9ad2e0442bf013062a284ae4f722	no	200
Warnings:					
Information:					
59	Non Patent Literature	D1367part59.pdf	5328626 36f13527af4c3ff03ecdfb50c9414156531caa1f	no	200
Warnings:					
Information:					
		Total Files Size (in bytes):	306483781		

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.

1897932

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

September 21, 2012

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY OF

REEXAMINATION CERTIFICATE NUMBER 6,502,135 C1, CERTIFICATE ISSUED JUNE 07, 2011.

By Authority of the

Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office

P. SWAIN

Certifying Officer

Plaintiffs' VirnetX Exhibit

VirnetX, Inc. v. Apple, Inc.

PX558

C.A. 6:10-cv-0417

VX00690594

(12) **INTER PARTES REEXAMINATION CERTIFICATE** (0271st)

United States Patent

Munger et al.

(10) **Number: US 6,502,135 C1**

(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

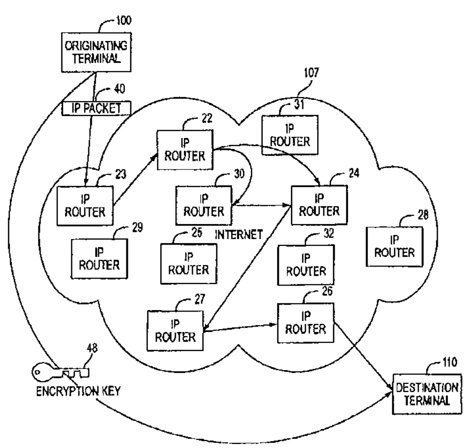
Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/draft302.txt on Feb. 4, 2002, 56 pages.

(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	Caimi
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). (DNSSEC–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 WinInet* 313–423 (Addison Wesley Longman 1998) (Essential WinInet).
Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) available at http://msdn2.microsoft.com/enus/library/ms811078 (printer).aspx (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 Adminstrator'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).

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. Matehrs 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/19997062003l945/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

* * * * *

Electronic Acknowledgement Receipt

EFS ID:	14975799
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-FEB-2013
Filing Date:	23-DEC-2011
Time Stamp:	21:00:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1323.pdf	1422687 5053f6e89628e87a76c4cad00df2c78c6a197e8f	no	3

Warnings:

Information:

2	Non Patent Literature	D1324.pdf	1657880 35edfc131d77ab0ec4d915dba45b1baf861 8fb7e	no	3
Warnings:					
Information:					
3	Non Patent Literature	D1325.pdf	1652566 4aac9ad54146c0b212453a0fb40c0302131 15806	no	2
Warnings:					
Information:					
4	Non Patent Literature	D1326.pdf	1606446 43858fe22b54c055fa9910bc4048b656fd73 cefd	no	2
Warnings:					
Information:					
5	Non Patent Literature	D1327.pdf	1628105 79d0de0afe3ba9df8d2e319e29b95bf6e3b 2438b	no	2
Warnings:					
Information:					
6	Non Patent Literature	D1328.pdf	1660574 a66b2834af80d0b20b1232eae9c600c8c01 b3da8	no	3
Warnings:					
Information:					
7	Non Patent Literature	D1329.pdf	165761 2799ce86b9fb02f2610fd05e68b5c10d5792 9e46	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:					
8	Non Patent Literature	D1330.pdf	1528953 90841abd2aec80fd7db54dc354ba7471f1a 537df	no	1
Warnings:					
Information:					
9	Non Patent Literature	D1331.pdf	1881993 525fd869875fc8b21e23fe137d6f9f10d4435 26b	no	4
Warnings:					
Information:					
10	Non Patent Literature	D1332.pdf	4208513 628abf59dd7c687a820cea0cc1221333b6d a55f7	no	49

Warnings:

Information:

11	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:

12	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:

13	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:

14	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:

15	Non Patent Literature	D1337.pdf	1693967 86bc65b9e9ce85091006dfde1b751d20d77db78b	no	4

Warnings:

Information:

16	Non Patent Literature	D1338.pdf	1010871 8cd58e8c9a621ebb661db8c15d35495c3eced84c	no	1

Warnings:

Information:

17	Non Patent Literature	D1339.pdf	1361716 76ae31ebed6a611e46ac7fd2fc480fa1c01043dc	no	4

Warnings:

Information:

18	Non Patent Literature	D1340.pdf	117551 9f3ccab33733fb8b4c91aeb24869af488793 3b5e	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:					
19	Non Patent Literature	D1341.pdf	1586481 18c999d527a6e63e49a24243eb2848bba71 e3cbb	no	2
Warnings:					
Information:					
20	Non Patent Literature	D1342.pdf	4567422 33c7c83c8facdf6b1925227a9df809c2f45f5 d14	no	39
Warnings:					
Information:					
21	Non Patent Literature	D1343.pdf	1386522 fc6a4547b1e56c6f6ed6d1d9133e1dff8100 9fbf	no	128
Warnings:					
Information:					
22	Non Patent Literature	D1344.pdf	3224028 143baeeedb8e7fc279fc796714845fc22ce8 3bc1	no	27
Warnings:					
Information:					
23	Non Patent Literature	D1345part3.pdf	9257367 9e07a4f4e2e1e05ec1172bd0dfa7083598d a7e71	no	150
Warnings:					
Information:					
24	Non Patent Literature	D1345part4.pdf	10336191 1c01b8ccdec738f5c0c088bfc2b0cf22ad1f1 31a	no	150
Warnings:					
Information:					
25	Non Patent Literature	D1345part5.pdf	8946138 f05004993463461699993af6370a7710d0d9 cb30d	no	150
Warnings:					
Information:					
26	Non Patent Literature	D1345part6.pdf	8828613 099ca1650d1b9f5b7c2459058c6346b1d11 1d55e	no	150

Warnings:					
Information:					
27	Non Patent Literature	D1345part7.pdf	8560141 e6bd414516d47087f599aab3f308622e8283df52	no	150
Warnings:					
Information:					
28	Non Patent Literature	D1345part8.pdf	9356808 af3313861cd5f9b729d178896b769ed4455f4162	no	150
Warnings:					
Information:					
29	Non Patent Literature	D1345part9.pdf	9764625 64b894c3184974d20bebd232d095bb54bd010a6b	no	150
Warnings:					
Information:					
30	Non Patent Literature	_D1345part1.pdf	8057998 f47dae52b5279e5071879b2230170c2d849dcbd3	no	100
Warnings:					
Information:					
31	Non Patent Literature	_D1345part2.pdf	7593970 5b5c0726510c37610f7563687de708e4389bb895	no	100
Warnings:					
Information:					
32	Non Patent Literature	_D1345part10.pdf	1423238 596a082b8447685e7dfd212ffde96e40bcebc406	no	150
Warnings:					
Information:					
33	Non Patent Literature	D1346.pdf	1919004 a749b23be1d527cdca70d02fdf7ec267c9b48f7c	no	3
Warnings:					
Information:					
34	Non Patent Literature	D1347.pdf	1497286 5782c123c01822cd82847467cc58c1549d2893d4	no	3
Warnings:					
Information:					
35	Non Patent Literature	D1348.pdf	3063828 e518be7623faedbcec17d1bb276de1240aa5b5c2	no	36

Warnings:					
Information:					
36	Non Patent Literature	D1349.PDF	1286364 958865142a880cea138f87b5c810c0f1df4fc639	no	4
Warnings:					
Information:					
37	Non Patent Literature	D1350.pdf	1315534 15e30298a1660e16fb614885f43a9935befda828	no	3
Warnings:					
Information:					
38	Non Patent Literature	D1351.pdf	3078803 a08178b7efe18b87b23e63f3d061cc3e44699c99	no	22
Warnings:					
Information:					
39	Non Patent Literature	D1352.pdf	7439047 d9da5167524e9d452a1feccd1bede7f2d4c483f3	no	116
Warnings:					
Information:					
40	Non Patent Literature	D1353.pdf	739926 b3492a5af9e4cd344c7af5263b9f55ac4fb6e4c6	no	6
Warnings:					
Information:					
41	Non Patent Literature	D1355.pdf	1862178 10c4110f046b1dc6bae52b1113396432015cf1f7	no	10
Warnings:					
Information:					
42	Non Patent Literature	D1356.pdf	1878558 ccd50a0a173c9affbe903665d792c92a3747785a	no	30
Warnings:					
Information:					
43	Non Patent Literature	_D1357part1.pdf	5635558 fc0d484bb31d0e28d64109585b1a6e96c00024b6	no	75
Warnings:					
Information:					
44	Non Patent Literature	_D1357part2.pdf	6501603 05b00a3e30d50a8516972eef0cb54974f6ef7cfb	no	75

Warnings:					
Information:					
45	Non Patent Literature	D1357part3.pdf	6588852 f6f10620ebd2e192978388711f6f57685c729f35	no	75
Warnings:					
Information:					
46	Non Patent Literature	D1357part4.pdf	6656277 7511c7477a1f1629d4d1bf47899c553d9de6e564	no	75
Warnings:					
Information:					
47	Non Patent Literature	D1357part5.pdf	5013231 8704bd7b294bdbe6af4a451be202c667077bc92f	no	56
Warnings:					
Information:					
48	Non Patent Literature	D1354.pdf	139202 a1a19c125aa4b950132854f4c88d98a1550cc064	no	68
Warnings:					
Information:					
49	Non Patent Literature	D1358.pdf	1459176 09af3d6fa978700a4183ee42d3defabc8dc0c6fd	no	9
Warnings:					
Information:					
50	Non Patent Literature	D1360.pdf	2039339 fa1e4f7f58a54caaf7839afd2e2ea65a0731ed52	no	8
Warnings:					
Information:					
51	Non Patent Literature	D1361.pdf	618909 e511497cba6683792a8519d5a04ac45bb1461166	no	5
Warnings:					
Information:					
52	Non Patent Literature	D1366.pdf	2675465 faa218677b0b25f03b26af98f7e0f1feb868e360	no	11
Warnings:					
Information:					
53	Non Patent Literature	D1362.pdf	373586 22c4361dfd74c3b6fa4eea0d570fc87e8212e37c	no	3

Warnings:					
Information:					
54	Non Patent Literature	D1363.pdf	686232 08fc3a5de12cee958594ad4dc03e1b8c883c72ad	no	6
Warnings:					
Information:					
55	Non Patent Literature	D1364.pdf	83229 7f8cb9e409de8c4514fd60a5389d27355b89a7d8	no	1
Warnings:					
Information:					
56	Non Patent Literature	D1365.pdf	55043 5d7dc77c413956d0fdad7ea3c1680d1777c49e59	no	17
Warnings:					
Information:					
57	Non Patent Literature	D1359.pdf	53296 9613954f4f62b572a41c199011e31d85da45bd65	no	5
Warnings:					
Information:					
		Total Files Size (in bytes):	184594959		

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:	14975215
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-FEB-2013
Filing Date:	23-DEC-2011
Time Stamp:	21:02:04
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	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:

2	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:

3	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:

4	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:

5	Non Patent Literature	D1287.pdf	10963972 3792950038841ee39f79c39e4344dfded6424340	no	230

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	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:

7	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:

8	Non Patent Literature	D1290.pdf	1190467 761affb6394261888853f2f445d4710c0ed7866c	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:

9	Non Patent Literature	D1291.pdf	1151230 2da3b15e0c77faf8f57601ba92c5f57e52d883b1	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:

10	Non Patent Literature	D1292.pdf	922465 7dc424353d785b3335d98a14a66adcb428636402	no	24

Warnings:

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

Information:

11	Non Patent Literature	D1293.pdf	770990 9d5192029566db32fdaf39bca241c6a7ab1ab2c3	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:

12	Non Patent Literature	D1294.pdf	3507569 4cf13095dff5a221b23ca701ed53a58f113959c8	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:

13	Non Patent Literature	D1295.pdf	2687595 0dea30cb6abe860acd764c0e12048643aec87ec1	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:

14	Non Patent Literature	D1296.pdf	511028 fe8d7387a99508be8688db79287719917280f310	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:

15	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:

16	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:

17	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:

18	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:

19	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:

20	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:

21	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:

22	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:

23	Non Patent Literature	D1305.pdf	1639377 3f2ee4e30b0d8277286c9589d857a6ed57179850	no	3

Warnings:

Information:

24	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:

25	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:

26	Non Patent Literature	D1308.pdf	1713912 5d3b52c468d964a44056235ce0f19346b43bdfa1	no	3

Warnings:

Information:

27	Non Patent Literature	D1309.pdf	4837212 71cd505e05ee38db05e0c80e55c42915f07d2254	no	26

Warnings:

Information:

28	Non Patent Literature	D1310.pdf	1726922 f687bf9fc6f27805c1db848b7fb02ff172cbeeb1	no	3

Warnings:

Information:

29	Non Patent Literature	D1311.pdf	401591 11973f6357e29088a2eb474659dc28eae649e1a2	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:

30	Non Patent Literature	D1312.pdf	2108729 451d9ff1453b51f9c61d46baed16e6fce3e7523c	no	5

Warnings:

Information:

31	Non Patent Literature	D1313.pdf	63776 6821b85fea68253b4b9cdb3204b7f32aab9a57d9	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:

32	Non Patent Literature	D1314.pdf	1542980 31b4f75f9eeea7ddd051716ba894e2be65b2ac05	no	2

Warnings:

Information:

33	Non Patent Literature	D1315.pdf	1329379 b2ec3b27189c0fe0de9d1c4718c1df4190ce4120	no	2

Warnings:

Information:

34	Non Patent Literature	D1316.pdf	623682 94076e48f82f7eccae0329b5dab209050dd2b73f	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:

35	Non Patent Literature	D1317.pdf	2160424 e924afcfef661b92945145fba4a6c94bcc15f7a2	no	4

Warnings:

Information:					
36	Non Patent Literature	D1318.pdf	2036652 2766ec5cf4861facd5686a94d55974010394c648	no	8
Warnings:					
Information:					
37	Non Patent Literature	D1319.pdf	1606014 2ce01a101c40f94b7b8a7c81f68508083e548737	no	2
Warnings:					
Information:					
38	Non Patent Literature	D1320.pdf	1689282 b7798cf17288dc3acb9307706c2a2a70973f184c	no	3
Warnings:					
Information:					
39	Non Patent Literature	D1321.pdf	1910327 e76ea173ade25cb899279ee9a0b4afe126acedd7	no	3
Warnings:					
Information:					
40	Non Patent Literature	D1322.pdf	1626309 514ab682b932d58d61a827a2118ddf49698bba89	no	5
Warnings:					
Information:					
		Total Files Size (in bytes):	87170518		

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:	14977167
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-FEB-2013
Filing Date:	23-DEC-2011
Time Stamp:	20:59:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1367part1.pdf	15960835 fe4eac6ef853165892de444e6b46f9c8b294 1991	no	201

Warnings:

Information:

2	Non Patent Literature	D1367part2.pdf	3171465 d41604ab63c8e5aaac499ffead29d43cbeb1f4ae	no	200
Warnings:					
Information:					
3	Non Patent Literature	D1367part3.pdf	3067154 eb4e223c50a6efb9b76ad963ca690fc0e148a696	no	200
Warnings:					
Information:					
4	Non Patent Literature	D1367part4.pdf	2754394 27542e3bfcef4163e8eaf027c3f59b3522719945	no	200
Warnings:					
Information:					
5	Non Patent Literature	D1367part5.pdf	3204769 b84f42ec4c8b3735e9e1d10456b0a4239b698cf5	no	200
Warnings:					
Information:					
6	Non Patent Literature	D1367part6.pdf	3562036 b5ea9c4993f34b249ce1de35548d1a328853a064	no	200
Warnings:					
Information:					
7	Non Patent Literature	D1367part7.pdf	3193057 2f0b7e75e2d4676116207937450bd355799f6882	no	200
Warnings:					
Information:					
8	Non Patent Literature	D1367part8.pdf	1736291 5c12f84a88ac4f0b839ca6d18800ccaa2ed770b3	no	200
Warnings:					
Information:					
9	Non Patent Literature	D1367part9.pdf	2778626 997661c418a9b95eb9fd80feb03c6537e59b2ea2	no	200
Warnings:					
Information:					
10	Non Patent Literature	D1367part10.pdf	2220634 136cee2ab62a09694855b9e5026450a12dc45ebf	no	200
Warnings:					
Information:					

11	Non Patent Literature	D1367part11.pdf	2896543 ccfb4ec5c7678f0697fad134148b0a51ef69ec5c	no	200
Warnings:					
Information:					
12	Non Patent Literature	D1367part12.pdf	3275415 54a76826c8a38b1d8d69ba5ca6b12edb294deee3	no	200
Warnings:					
Information:					
13	Non Patent Literature	D1367part13.pdf	2574446 1540300550e6afb5ffabffd0b1702c7bcc47e835	no	200
Warnings:					
Information:					
14	Non Patent Literature	D1367part14.pdf	2870775 33427066647a8efc1b58131ff552d2d39f6cf66c	no	200
Warnings:					
Information:					
15	Non Patent Literature	D1367part15.pdf	3533177 ce6ef0c77a5b674f2eb7a16d8c0b405f4ea9cf3d	no	200
Warnings:					
Information:					
16	Non Patent Literature	D1367part16.pdf	3786071 9784e33a377b4c0ed3296f46a47d237535a4b80f	no	200
Warnings:					
Information:					
17	Non Patent Literature	D1367part17.pdf	2829552 30217a4cf275dc8b68bc609bf783995807a1689f	no	200
Warnings:					
Information:					
18	Non Patent Literature	D1367part18.pdf	2742291 ca4f5a259b8536daa36b8b9ad409f5a1f1f09a66	no	200
Warnings:					
Information:					
19	Non Patent Literature	D1367part19.pdf	2846638 f69ee9b2ba78513e2b92bd0475d69e6a0fb4abc8	no	200
Warnings:					
Information:					

20	Non Patent Literature	D1367part20.pdf	2598677 de08e1f6b55e257936f24575e7fb5b954f37ee49	no	200
Warnings:					
Information:					
21	Non Patent Literature	D1367part21.pdf	3094007 0e0337954535cbbd5c5f97f2ec0ed5f8b5aa5116	no	200
Warnings:					
Information:					
22	Non Patent Literature	D1367part22.pdf	2473740 bb73365c8ef0c521ea22a11451b039e2c73a2672	no	200
Warnings:					
Information:					
23	Non Patent Literature	D1367part23.pdf	1839430 b40eec3f85e92e6fc9a6665e9f4bbd47672ef115	no	200
Warnings:					
Information:					
24	Non Patent Literature	D1367part24.pdf	2109084 55a0beaf6a686ba1cf800865faf64f519baf0f0b	no	200
Warnings:					
Information:					
25	Non Patent Literature	D1367part25.pdf	2066586 aa9ffa2f6eefa7f5c068f45a8ed0bd414648910a	no	199
Warnings:					
Information:					
26	Non Patent Literature	D1367part26.pdf	7803999 15026aae52ef28e0260fc2f06a4c7aa844abdc29	no	200
Warnings:					
Information:					
27	Non Patent Literature	D1367part27.pdf	6949434 4431b64464736425547db671b1f533059c60ae74	no	200
Warnings:					
Information:					
28	Non Patent Literature	D1367part28.pdf	9420516 99f1bc77d51a1c0e59963be6e8125f62582b2d3b	no	200
Warnings:					
Information:					

29	Non Patent Literature	D1367part29.pdf	8622584 f52e7ff9af96e1be67fa0bf4e415c6edc884d6db	no	200
Warnings:					
Information:					
30	Non Patent Literature	D1367part30.pdf	5691420 aff21f5e3c4226b2942d8ea86909f27b84efeae4	no	200
Warnings:					
Information:					
31	Non Patent Literature	D1367part31.pdf	5147177 79a3fb072f1038c5a54619f42af13855c8d61095	no	200
Warnings:					
Information:					
32	Non Patent Literature	D1367part32.pdf	4989115 ff4eec8f363c85b9e96f09e060f053d2ad486b2a	no	200
Warnings:					
Information:					
33	Non Patent Literature	D1367part33.pdf	5568352 d9e1acef97040cfe5cf0175be4737a18634ccc13	no	200
Warnings:					
Information:					
34	Non Patent Literature	D1367part34.pdf	8490123 3dc07e6085f579298408aa4661548536d76d29a6	no	200
Warnings:					
Information:					
35	Non Patent Literature	D1367part35.pdf	6798116 70e0df0fd8749da37e86e377b2db6d4da47cda6f	no	200
Warnings:					
Information:					
36	Non Patent Literature	D1367part36.pdf	3485165 3eced5d52de48ba1800fe1f8ca4af5138044b82b	no	200
Warnings:					
Information:					
37	Non Patent Literature	D1367part37.pdf	4016005 20e974b5331b980e7d7eb529725eff12e8f04a4f	no	200
Warnings:					
Information:					

38	Non Patent Literature	D1367part38.pdf	3636004 fca83e506ae11779b35e45a8c9cffcfcec7dfc a1	no	200
Warnings:					
Information:					
39	Non Patent Literature	D1367part39.pdf	4305786 180e4c71fd02cc5906a2c19341d90b2c863 11ce1	no	200
Warnings:					
Information:					
40	Non Patent Literature	D1367part40.pdf	4903541 7f108e007a707311b614e8b6605f08c3ca92 3ed3	no	200
Warnings:					
Information:					
41	Non Patent Literature	D1367part41.pdf	7138830 72be8053f1ae72eb1cb9bd64705ffa64a059 e13a	no	200
Warnings:					
Information:					
			Total Files Size (in bytes):	180151860	

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.

No documents available for this priority number.

Espacenet

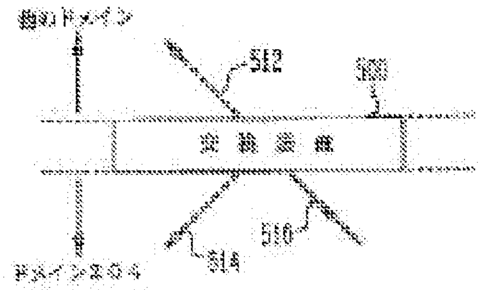
Bibliographic data: JP10111848 (A) — 1998-04-28

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）

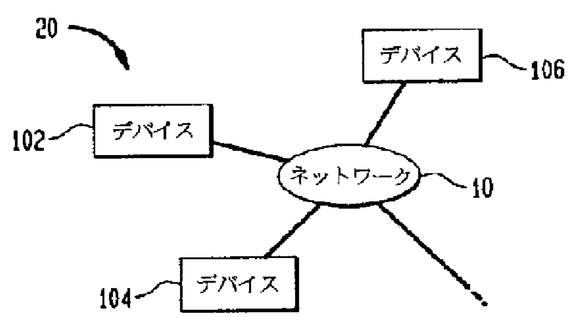
最終頁に続く

(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。

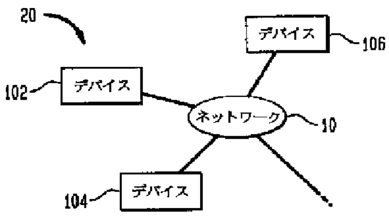
【００４３】図１０に示される実施形態は、照会要求をドメイン２０４外の適当なドメインネームサーバの代わりにＤＮＳプロキシ４０４に転送するレゾルバ１１２と１１４およびデバイス１１６のようなデバイスのソフトウェアの修正を必要とする。デバイス１１６はドメインネームサーバではなく、通信経路３２２を通じて直接外部情報源と通信する能力を有する。この実施形態では通信経路３１８、３２０および３２２は、ＤＮＳプロキシ４０４に転送される。

【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。

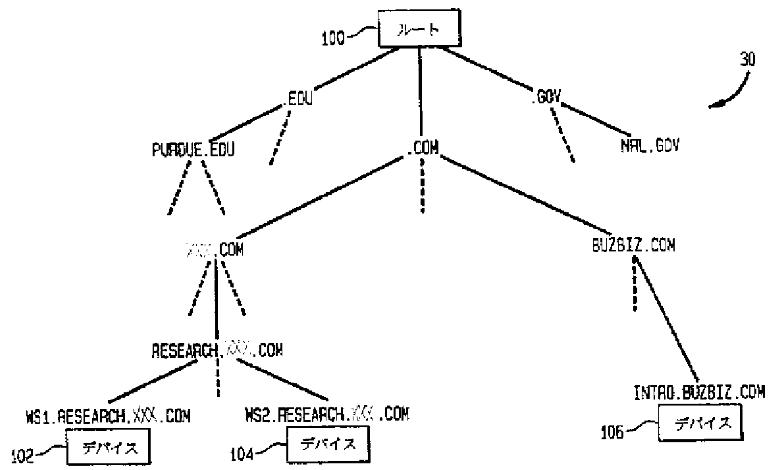
【００４５】通信経路３３０を通じて外部情報源から受信した情報も、ローカルセキュリティ保護管理ポリシーのために削除または修正される。例えば、外部情報源から受信した情報にドメイン２０４外のドメインネームサーバのポインタが含まれるならば、そのポインタは情報がドメイン２０４内の目的デバイスに送られる前に削除されなければならない。さもないと、ドメイン２０４内のデバイスが、こうしたドメインネームサーバにＤＮＳプロキシ４０４の介入なしに直接接触しようとすることがある。逆に、ドメイン２０４内のドメインネームサー

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。

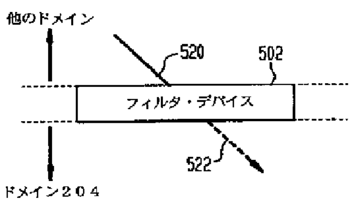
【図1】


20
デバイス
106
102
デバイス
ネットワーク
10
104
デバイス

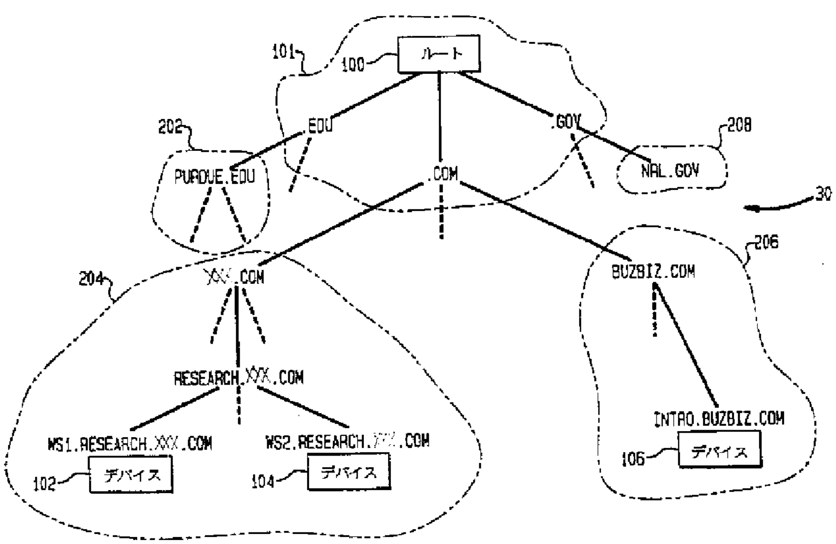
【図2】


100
ルート
30
.EDU
.GOV
PURDUE.EDU
.COM
NRL.GOV
.COM
BUZBIZ.COM
RESEARCH.
.COM
INTRO.BUZBIZ.COM
WS1.RESEARCH.XXX.COM
WS2.RESEARCH.
.COM
106
デバイス
102
デバイス
104
デバイス

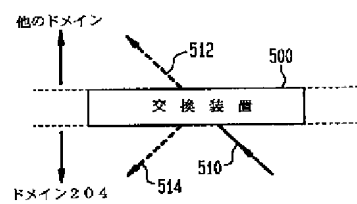
【図9】


他のドメイン
520
502
フィルタ・デバイス
522
ドメイン２０４

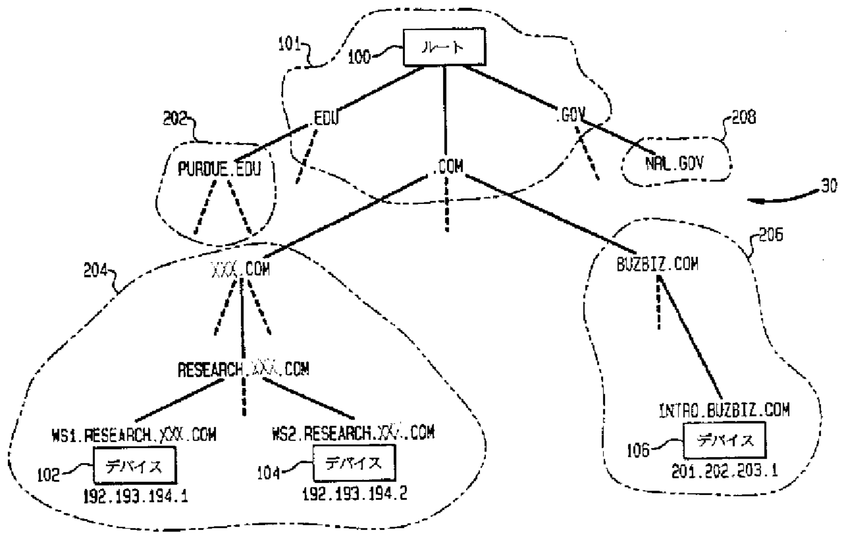
【図3】


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.
.COM
106
デバイス
102
デバイス
104
デバイス

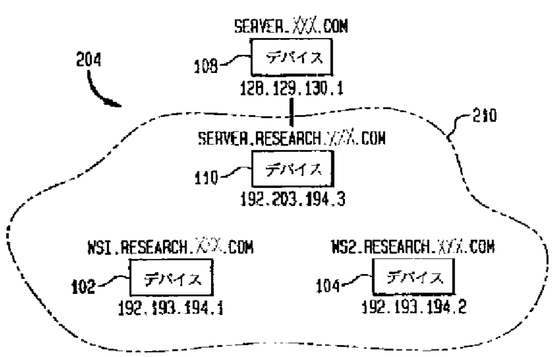
【図8】


他のドメイン
512
500
交 換 装 置
510
514
ドメイン２０４

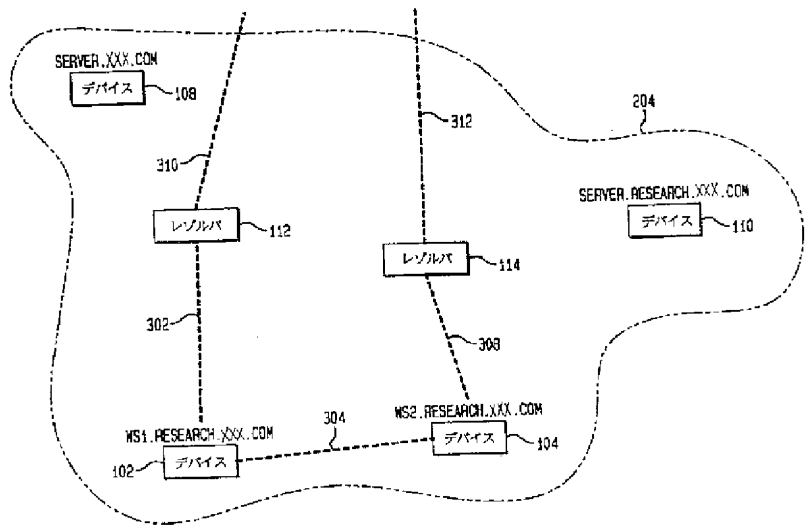
【図４】


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
102
デバイス
192.193.194.1
104
デバイス
192.193.194.2
INTRO.BUZBIZ.COM
106
デバイス
201.202.203.1

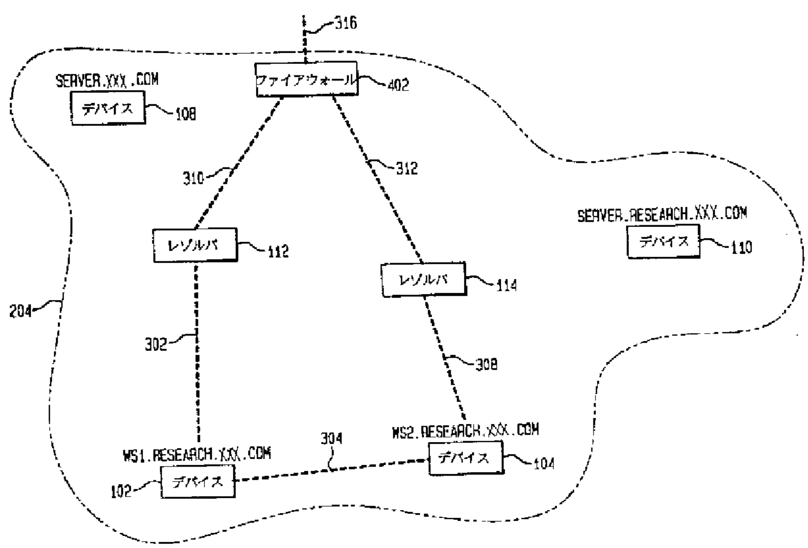
【図５】


SERVER.XXX.COM
204
108
デバイス
128.129.130.1
210
SERVER.RESEARCH.XXX.COM
110
デバイス
192.203.194.3
WS1.RESEARCH.XXX.COM
WS2.RESEARCH.XXX.COM
102
デバイス
192.193.194.1
104
デバイス
192.193.194.2

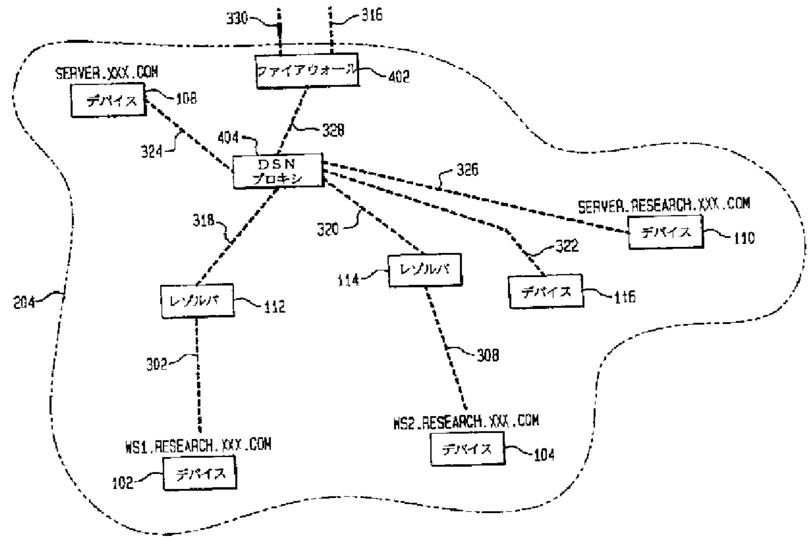
【図6】


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
WS1.RESEARCH.XXX.COM
デバイス
104
102
デバイス

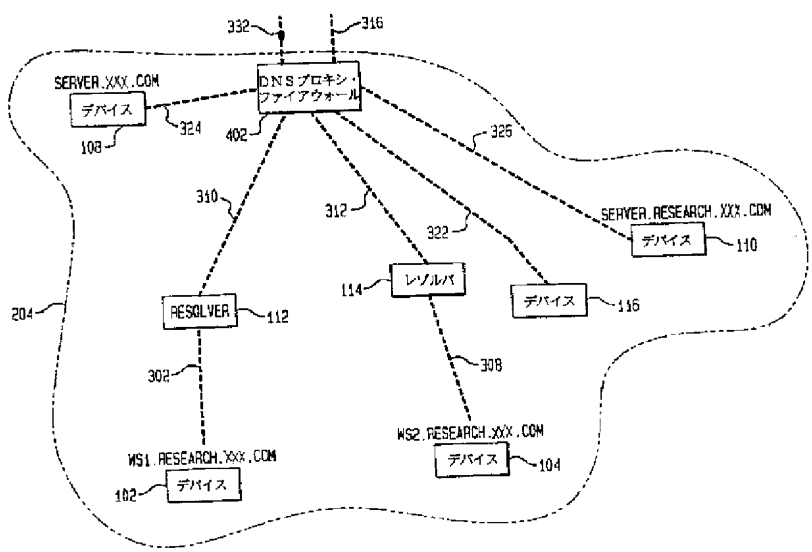
【図7】


316
SERVER.XXX.COM
ファイアウォール
402
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
WS1.RESEARCH.XXX.COM
デバイス
104
102
デバイス

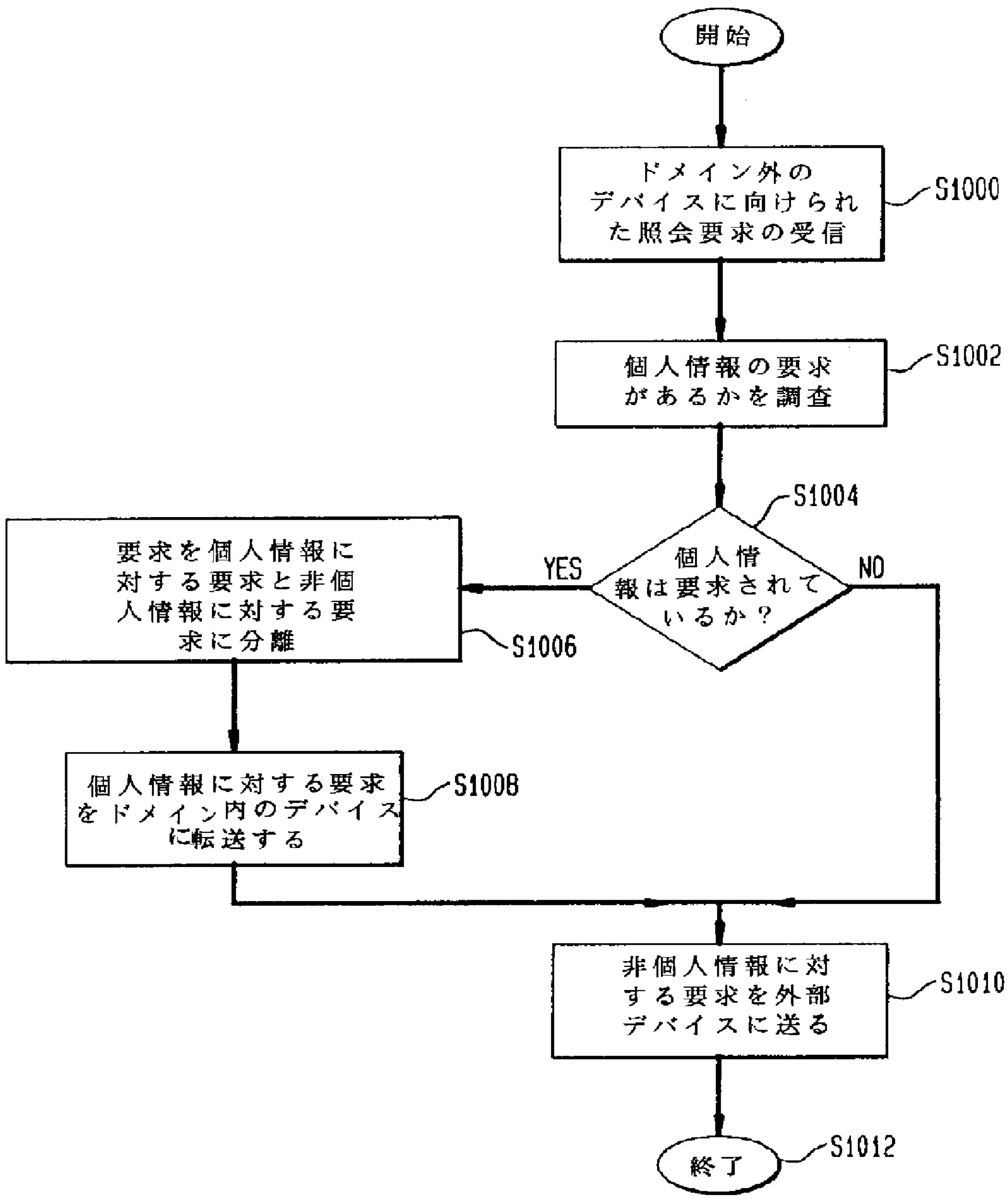
【図１０】


330
316
ファイアウォール
402
SERVER.XXX.COM
デバイス
108
328
404
324
DSN
プロキシ
326
SERVER.RESEARCH.XXX.COM
318
320
322
デバイス
110
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

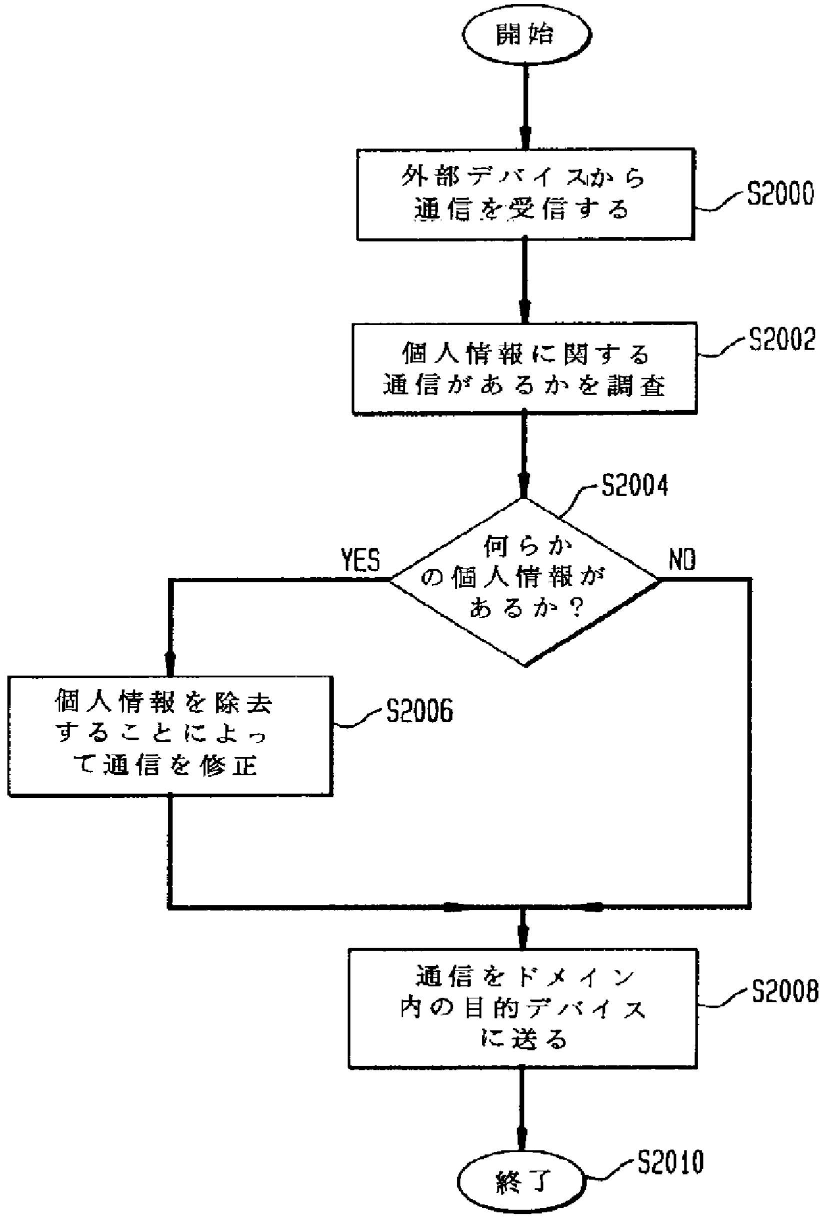
【図１１】


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
デバイス
116
204
RESOLVER
112
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**

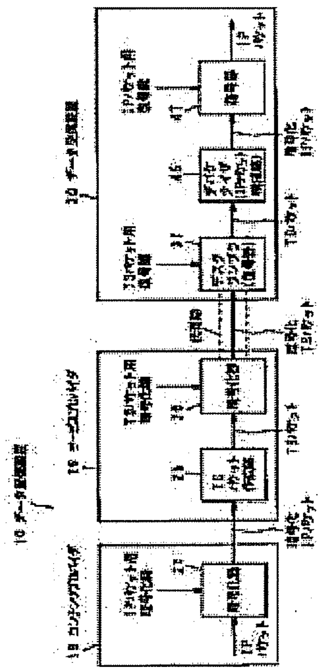
(30)Priority

Priority number : **08316726** Priority date : **27.11.1996** Priority country : **JP**

(71)Applicant : **SONY CORP**

(72)Inventor : **KUBOTA ICHIRO**
ASANO TOMOYUKI

(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	F I	
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

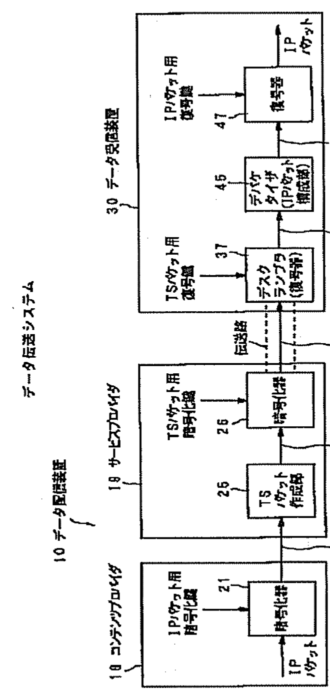
(74)代理人　弁理士　小池　晃　（外2名）

(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、デマルチプレクサ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。

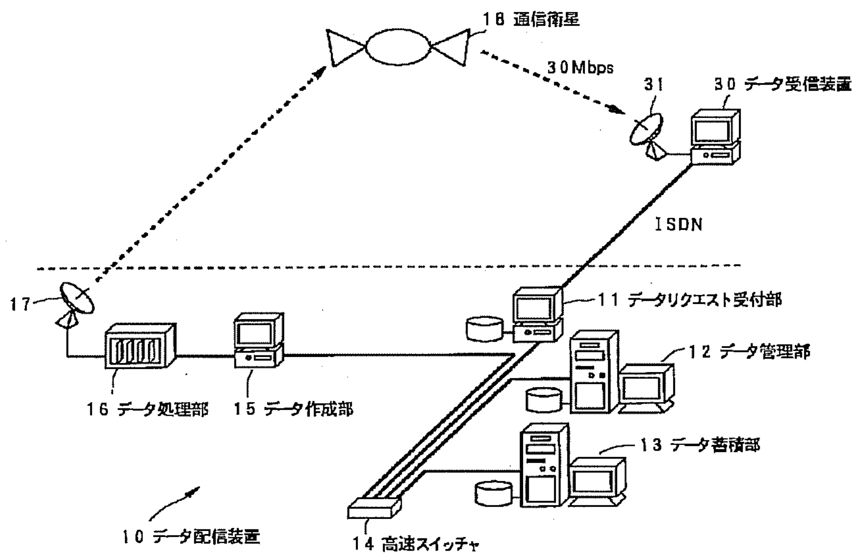
【図１６】上記データ伝送システム内のデータ受信装置の他の具体例を示すブロック図である。

【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。

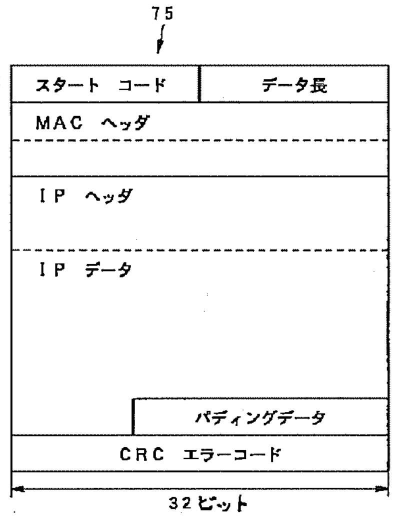
【符号の説明】

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

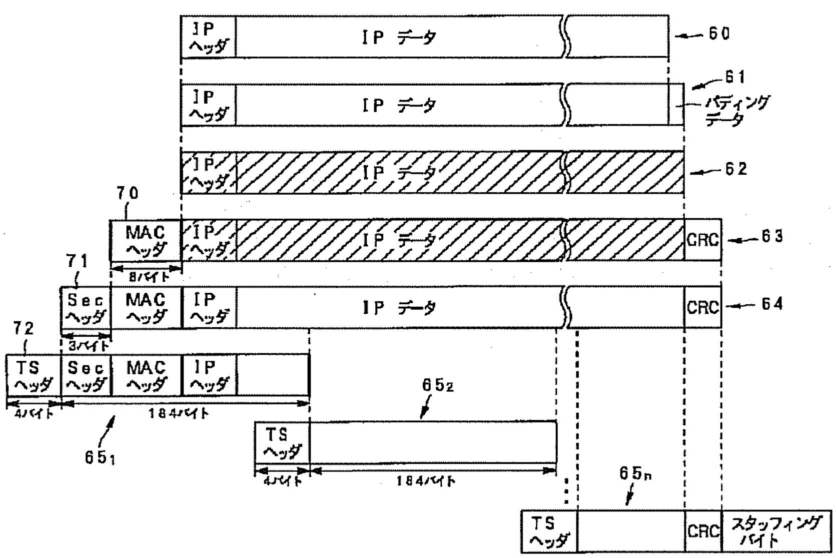
【図１】


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
16 データ処理部
15 データ作成部
13 データ蓄積部
10 データ配信装置
14 高速スイッチャ

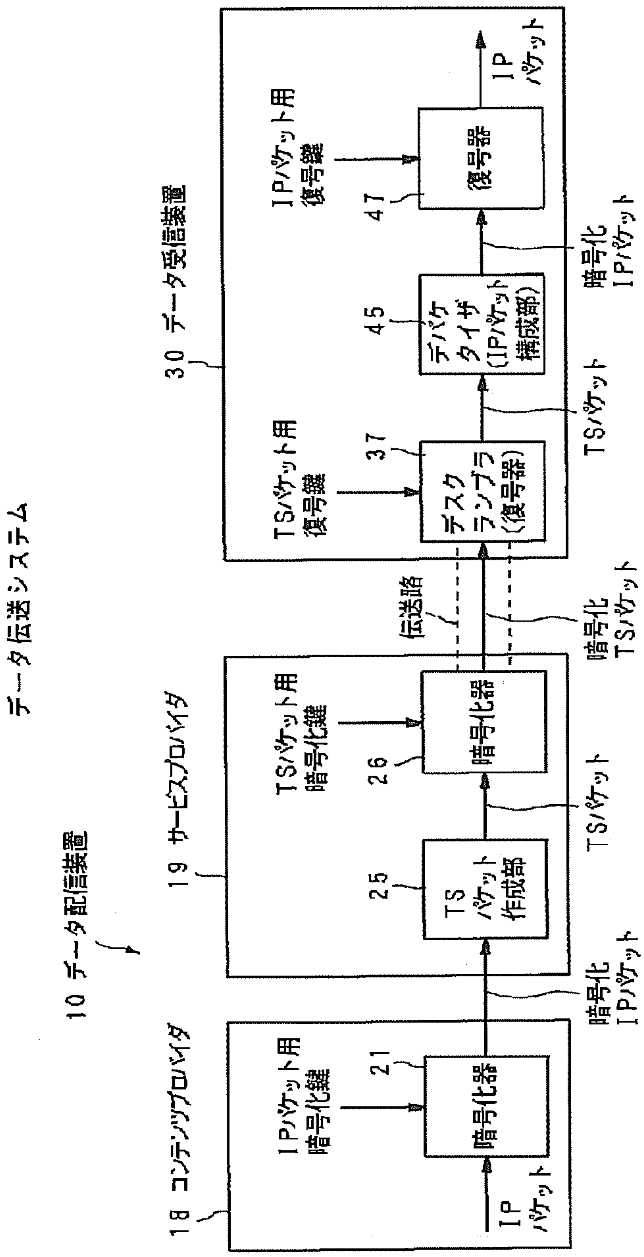
【図１０】


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

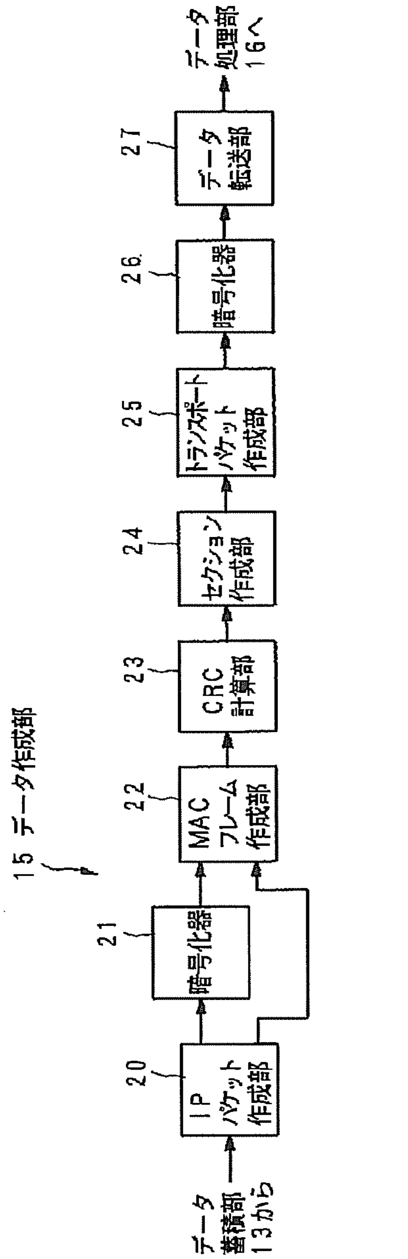
【図４】


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
65₁
65₂
65n
スタッフィング バイト

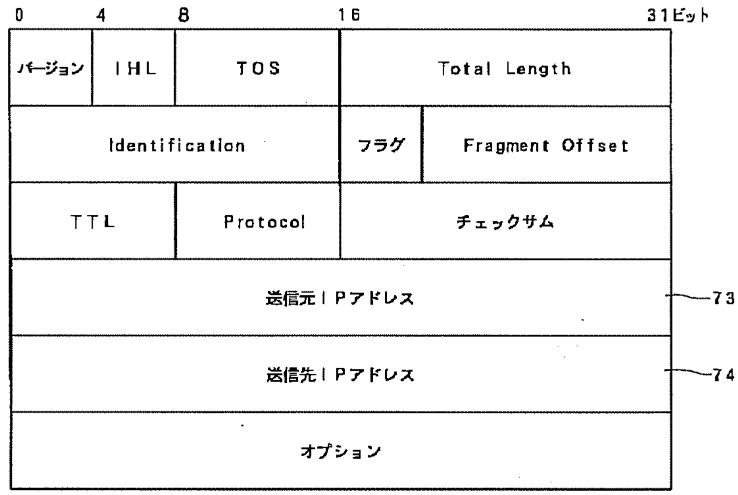
【図２】


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
伝送路
暗号化TSパケット
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

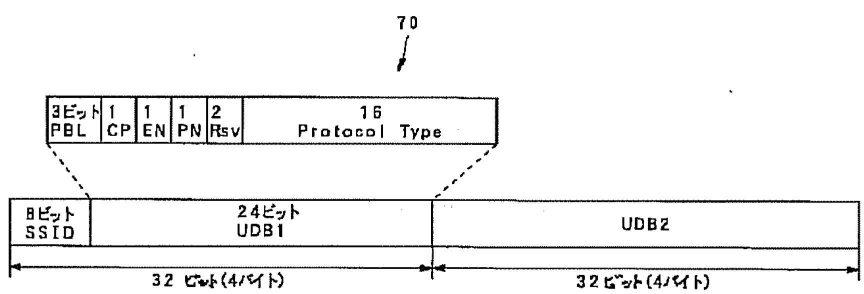
【図３】


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

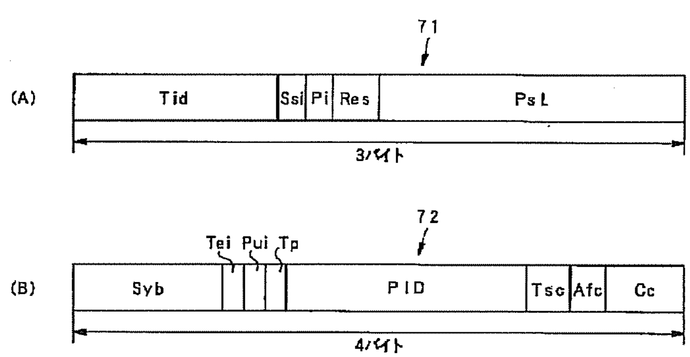
【図５】


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

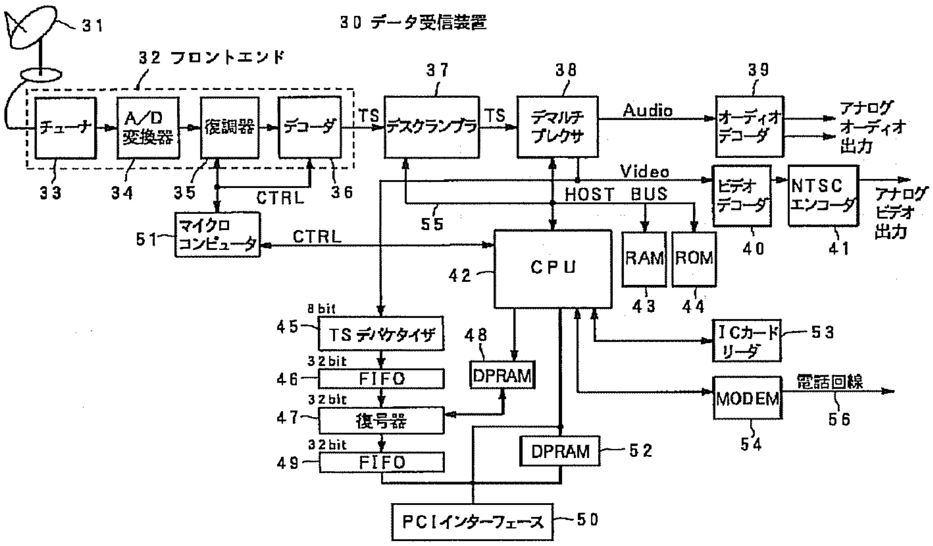
【図６】


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)

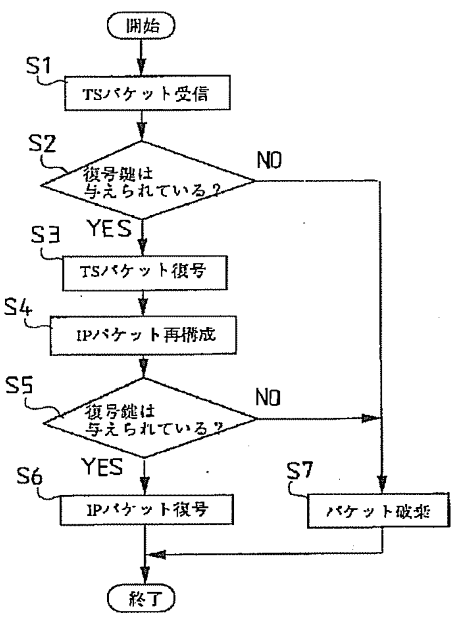
【図７】


71
(A)
Tid
Ssi
Pi
Res
PsL
3バイト
72
(B)
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】

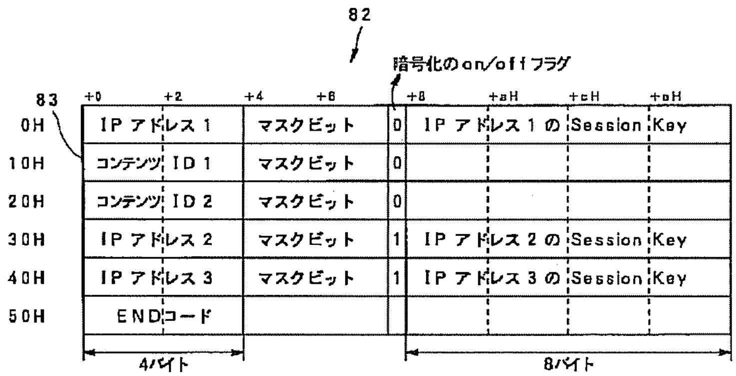
81

暗号化のon/offフラグ

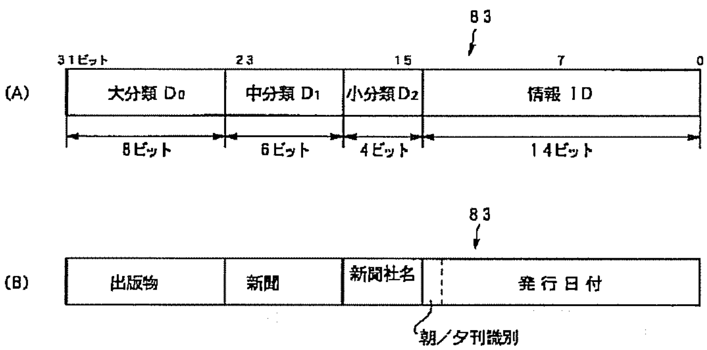
	+0	+2	+4	+6	フラグ	+8	+aH	+cH	+eH
0H	IP アド	レス 1	マスクビット		0	IP アド	レス 1 の	Session	Key
10H	IP アド	レス 2	マスクビット		1	IP アド	レス 2 の	Session	Key
20H	IP アド	レス 3	マスクビット		1	IP アド	レス 3 の	Session	Key
30H	IP アド	レス 4	マスクビット		1	IP アド	レス 4 の	Session	Key
40H	IP アド	レス 5	マスクビット		0	IP アド	レス 5 の	Session	Key
50H	END	コード							

4バイト　8バイト

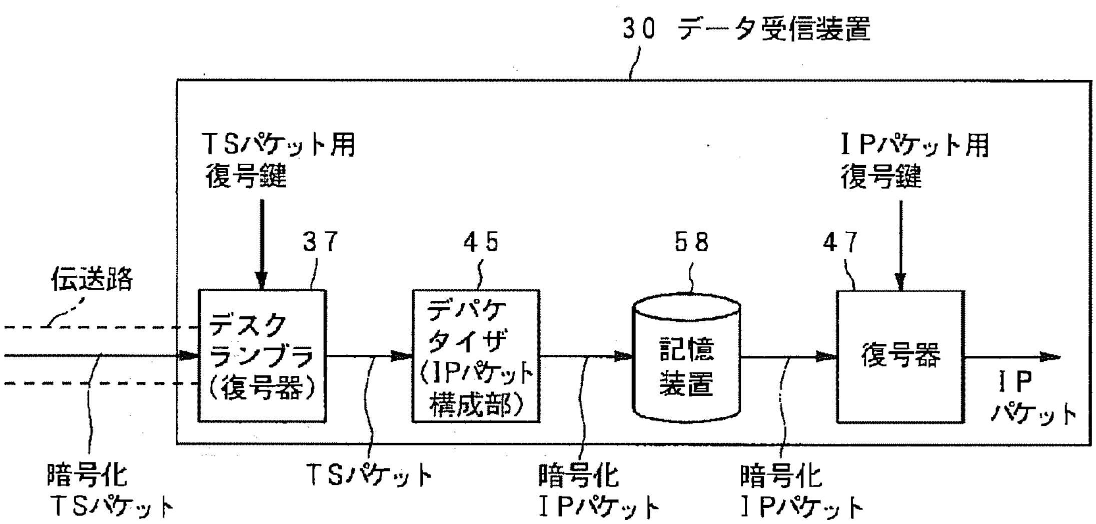
【図１３】


82
暗号化のon/offフラグ
83
+0 +2 +4 +6 +8 +aH +cH +eH
0H IPアドレス１ マスクビット 0 IPアドレス１のSession Key
10H コンテンツID１ マスクビット 0
20H コンテンツID２ マスクビット 0
30H IPアドレス２ マスクビット 1 IPアドレス２のSession Key
40H IPアドレス３ マスクビット 1 IPアドレス３のSession Key
50H ENDコード
4バイト
8バイト

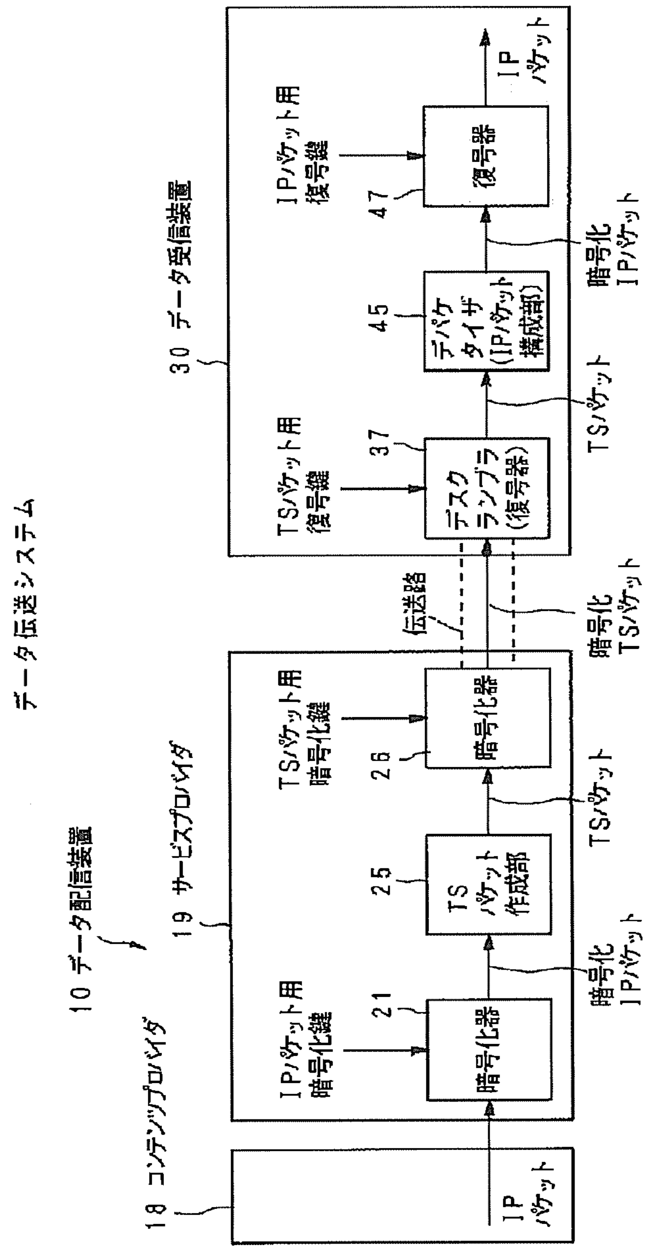
【図１４】


83
31ビット 23 15 7 0
(A) 大分類 D_0 中分類 D_1 小分類 D_2 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

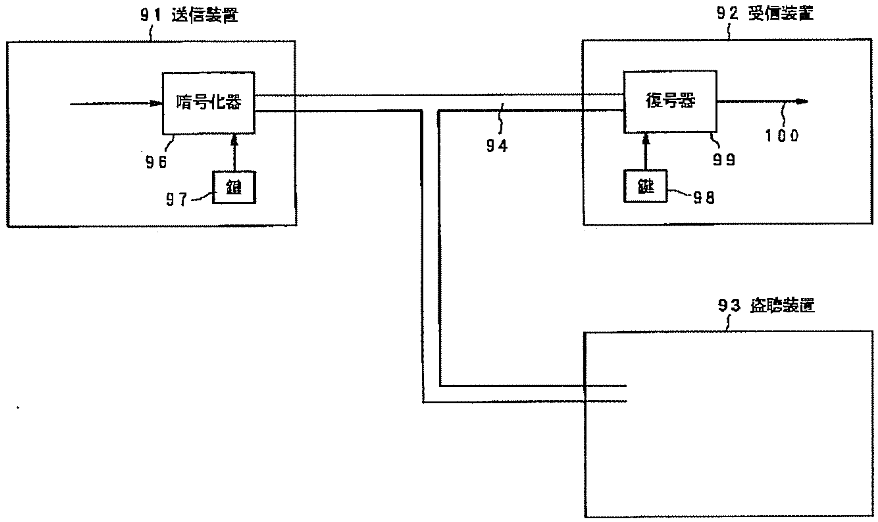
【図１６】


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
IP
パケット
19 サービスプロバイダ
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
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.

$K21 = C1^{r2 mod p}$

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

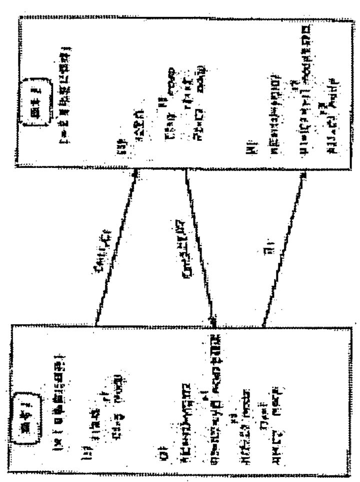
(21)Application number : **02-237498**

(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
㊿Int.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）

㊹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＞

（1）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、$y1=g^{x1} \bmod p$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、

$K12=y2^{x1} \bmod p=g^{x1 \times x2} \bmod p$

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、

$K21=y1^{x2} \bmod p=g^{x1 \times x2} \bmod p$

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)$Z12=y1^{r1} \bmod p$　　　・・・(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)$Z21=y2^{r2} \bmod p$　　　・・・(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。

$K21=(Z12 \times y1^{r2})^{x2} \bmod p$　・・・(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。

$K12=(Z21 \times y2^{r1})^{x1} \bmod p$　・・・(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。

$K12=(Z21 \times y2^{r1})^{x1} \bmod p=(y2^{r2+r1})^{x1} \bmod p=g^{x1 \times x2 \times (r1+r2)} \bmod p$

$K21=(Z12 \times y1^{r2})^{x2} \bmod p=(y1^{r2+r1})^{x2} \bmod p=g^{x1 \times x2 \times (r1+r2)} \bmod p$

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。

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

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。

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

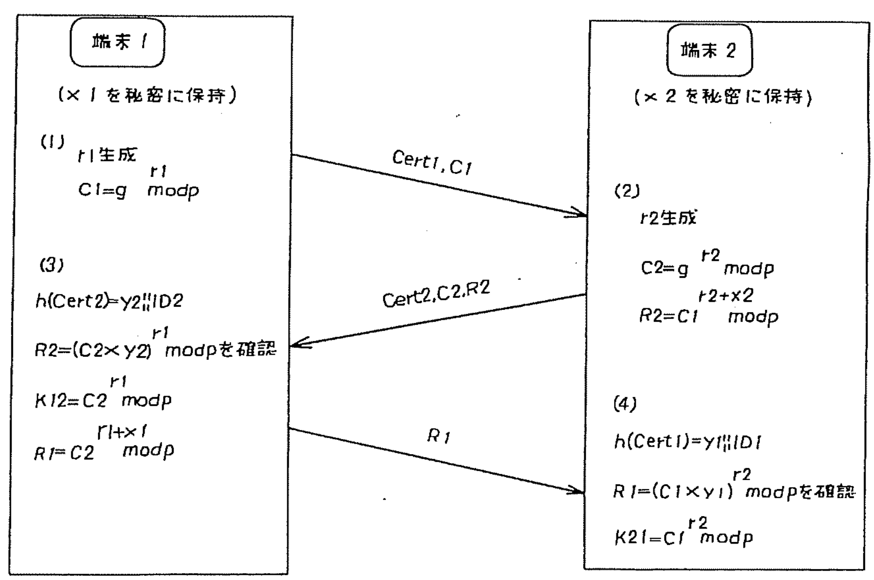
以上の説明から明らかなように本発明は、証明書を変更せずに毎回の共有鍵を変更することができる。また、相手を自身が発したチャレンジに対する応答を、センターの認めた相手の公開鍵を用いて直接的に確認する。チャレンジとレスポンスによる相手認証では、レスポンスに秘密の乱数を含めることによって端末の秘密情報を保護している。また、これにかかる計算量はべき乗剰余演算４回であり、間接的な認証しかできなかった従来の鍵配送方式と比べても最小限の計算量の増加となっている。

4．図面の簡単な説明

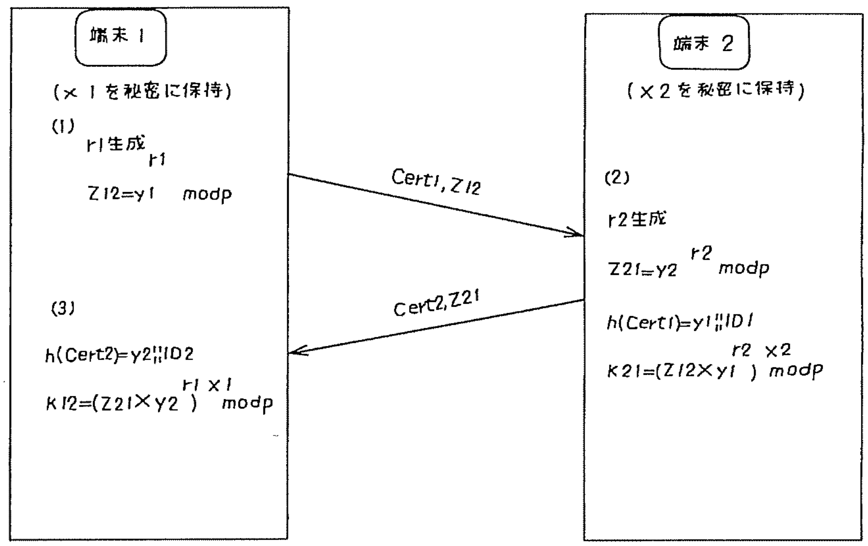
第１図は本発明の認証機能付き鍵配送方式における一実施例の鍵配送フェーズプロトコル図、第２図は従来における鍵配送フェーズプロトコル図である。

代理人の氏名　弁理士　小鍜治　明　ほか２名

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

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

September 18, 2012

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF:

U.S. PATENT: *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

R. PONDEXTER

Certifying Officer

Plaintiffs' VirnetX Exhibit

VirnetX Inc. v. Apple, Inc.

PX001

C.A. 6:10-cv-0417

VX00690521

US006502135B1

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

(10) **Patent No.: US 6,502,135 B1**
(45) **Date of Patent: Dec. 31, 2002**

(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: **Science Applications International Corporation**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/504,783**

(22) Filed: **Feb. 15, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999
(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.**[7] **G06F 15/173**
(52) **U.S. Cl.** **709/225**; 709/229; 709/245
(58) **Field of Search** 709/249, 223, 709/225, 229, 245; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE publication, 1996, pp. 963–967.

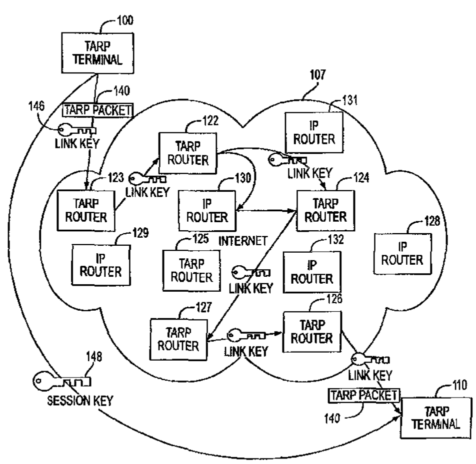
(List continued on next page.)

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

(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.

17 Claims, 35 Drawing Sheets



U.S. PATENT DOCUMENTS

5,588,060	A		12/1996	Aziz	
5,689,566	A		11/1997	Nguyen	
5,796,942	A		8/1998	Esbensen	
5,805,801	A		9/1998	Holloway et al.	
5,842,040	A		11/1998	Hughes et al.	
5,878,231	A	*	3/1999	Baehr et al.	709/243
5,892,903	A		4/1999	Klaus	
5,898,830	A	*	4/1999	Wesinger et al.	709/225
5,905,859	A		5/1999	Holloway et al.	
6,006,259	A		12/1999	Adelman et al.	
6,016,318	A	*	1/2000	Tomoike	370/338
6,052,788	A		4/2000	Wesinger, Jr. et al.	
6,079,020	A	*	6/2000	Liu	713/201
6,119,171	A		9/2000	Alkhatib	
6,178,505	B1	*	1/2001	Schneider et al.	713/168
6,226,751	B1	*	5/2001	Arrow et al.	370/351
6,243,749	B1		6/2001	Sitaraman et al.	
6,286,047	B1	*	9/2001	Ramanathan et al.	345/733
6,330,562	B1	*	12/2001	Boden et al.	707/10
6,332,158	B1	*	12/2001	Risley et al.	709/219
6,353,614	B1	*	3/2002	Borella et al.	370/389

OTHER PUBLICATIONS

Linux FreeS/WAN Index File, printed from http://liberty-.freeswan.org/freeswan_trees/freeswan–1.3/doc/ on Feb. 21, 2002, 3 pages.

J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freesswan–1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.

Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan/org/freeswan_trees/freeswan–1.3/doc/glossary.html on Feb. 21, 2002, 25 pages.

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

Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs—Research), "Crowds: Anonymity for Web Transactions", pp. 1–23.

Dolev, Shlomi and Ostrovsky, Rafail, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.

Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82–94.

Shree Murthy et al., "Congestion–Oriented Shortest Multipath Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028–1036.

Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1–14.

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

Search Report (dated Jun. 28, 2002), International Application No. PCT/US01/13261.

Donald E. Eastlake, "Domain Name System Security Extensions", DNS Security Working Group, Apr. 1998, 51 pages.

D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278–297 and pp. 351–375.

P. Srisuresh et al., "DNS extensions to Network Address Translators", Jul. 1998, 27 pages.

Laurie Wells, "Security Icon", Oct. 19, 1998, 1 page.

W. Stallings, "Cryptography And Network Security", 2^{nd} Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399–400.

W. Stallings, "New Cryptography and Network Security Book", Jun. 8, 1998, 3 pages.

* cited by examiner

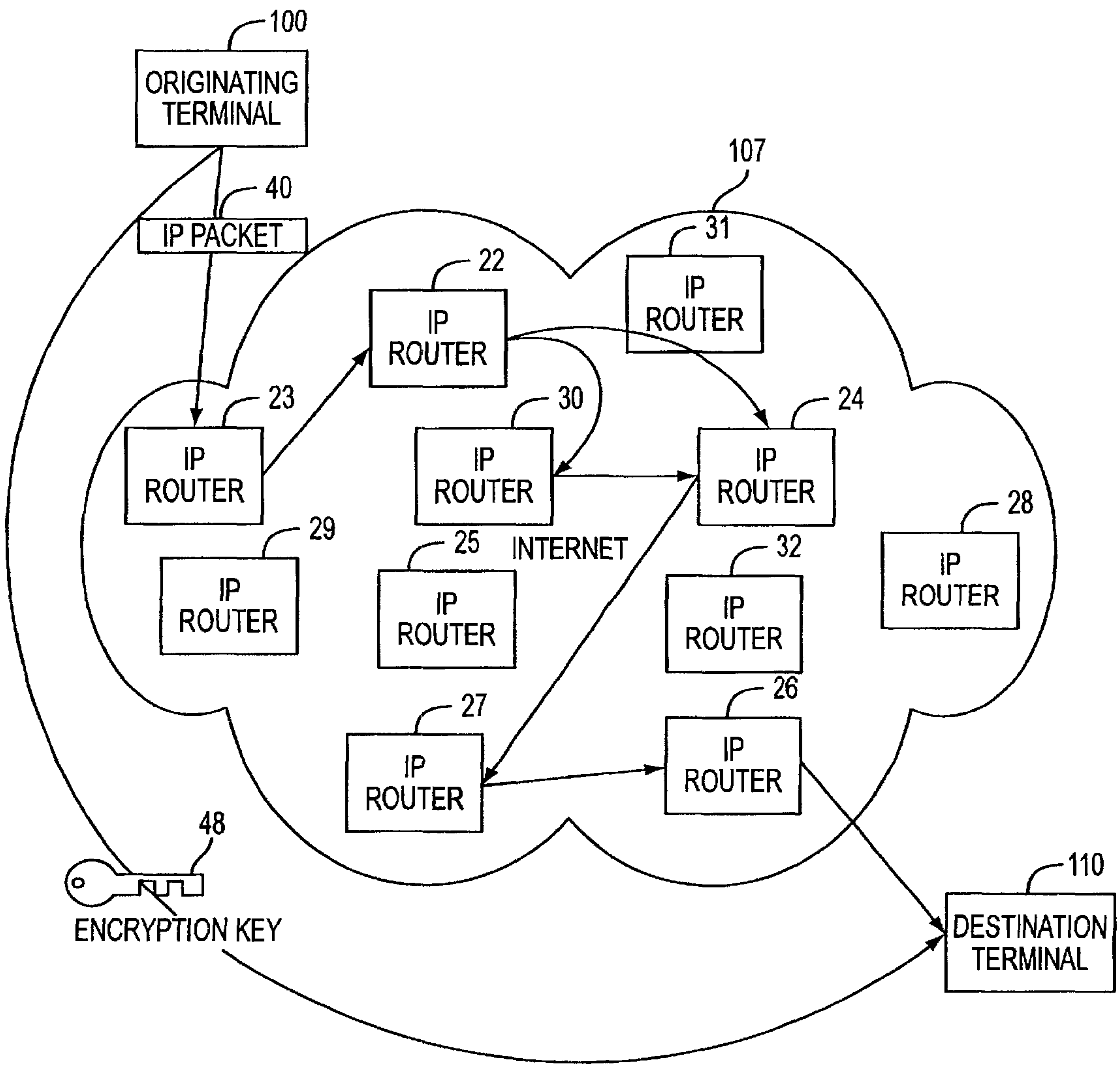

100
ORIGINATING TERMINAL
40
IP PACKET
107
31
IP ROUTER
22
IP ROUTER
23
IP ROUTER
30
IP ROUTER
24
IP ROUTER
28
IP ROUTER
29
IP ROUTER
25
IP ROUTER
INTERNET
32
IP ROUTER
27
IP ROUTER
26
IP ROUTER
48
ENCRYPTION KEY
110
DESTINATION TERMINAL

FIG. 1

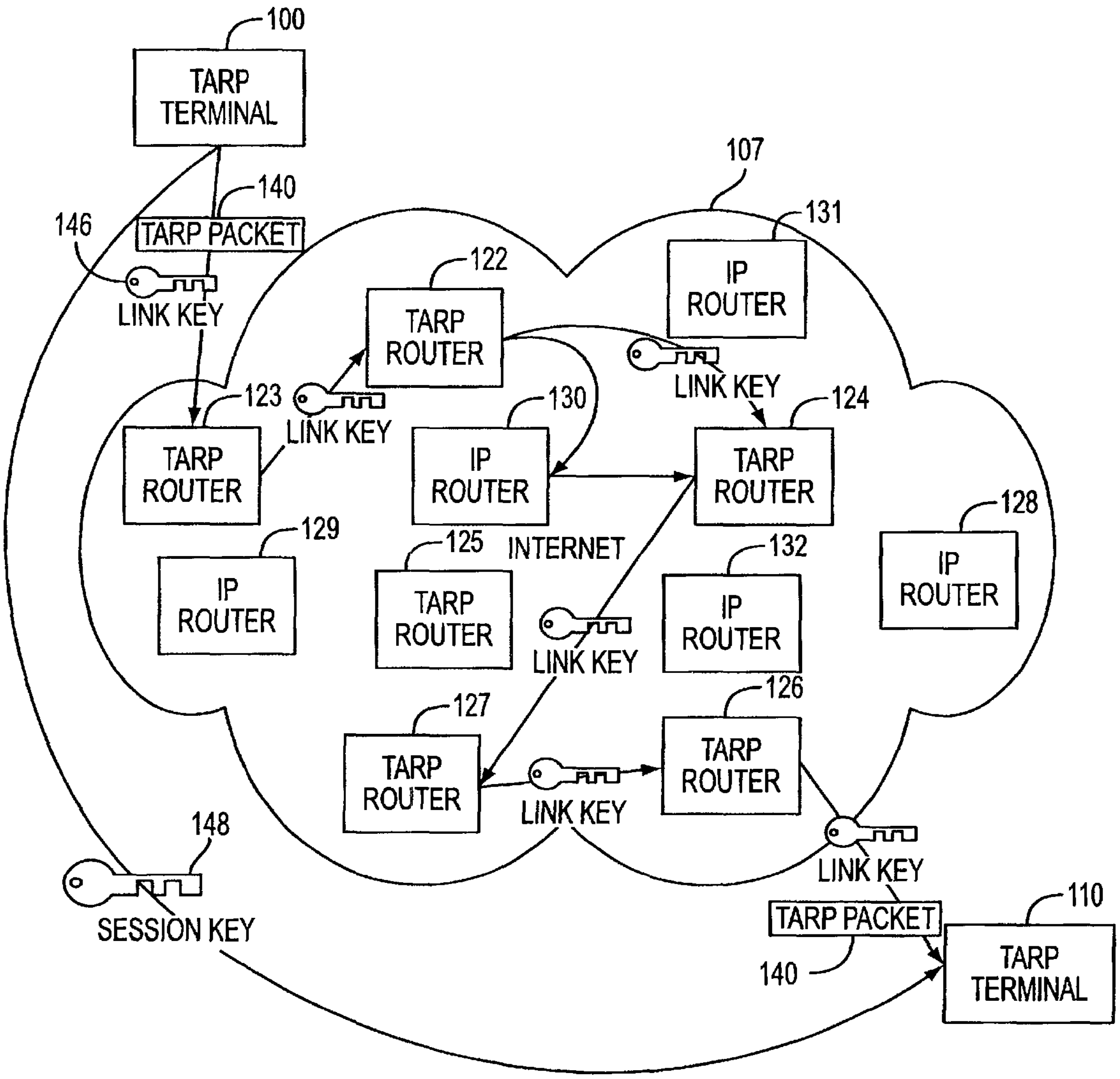

100
TARP TERMINAL
107
140
TARP PACKET
146
LINK KEY
131
IP ROUTER
122
TARP ROUTER
LINK KEY
123
TARP ROUTER
LINK KEY
130
IP ROUTER
124
TARP ROUTER
129
IP ROUTER
125
TARP ROUTER
INTERNET
132
IP ROUTER
128
IP ROUTER
LINK KEY
127
TARP ROUTER
126
TARP ROUTER
LINK KEY
148
SESSION KEY
LINK KEY
TARP PACKET
140
110
TARP TERMINAL

FIG. 2

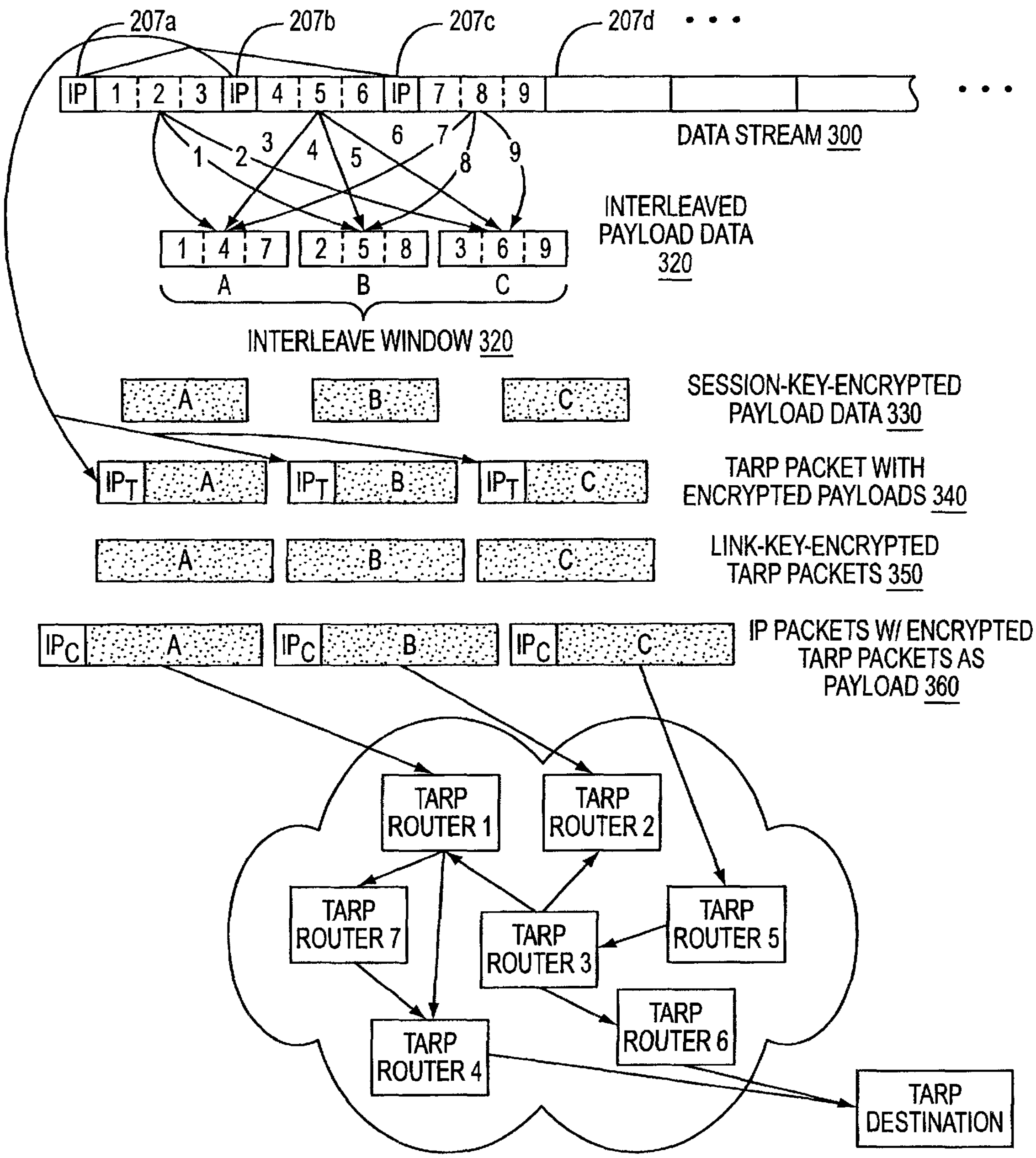

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
DATA STREAM 300
1 2 3 4 5 6 7 8 9
1 4 7
2 5 8
3 6 9
A B C
INTERLEAVED PAYLOAD DATA 320
INTERLEAVE WINDOW 320
SESSION-KEY-ENCRYPTED PAYLOAD DATA 330
TARP PACKET WITH ENCRYPTED PAYLOADS 340
LINK-KEY-ENCRYPTED TARP PACKETS 350
IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD 360
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 6
TARP ROUTER 4
TARP DESTINATION

FIG. 3A

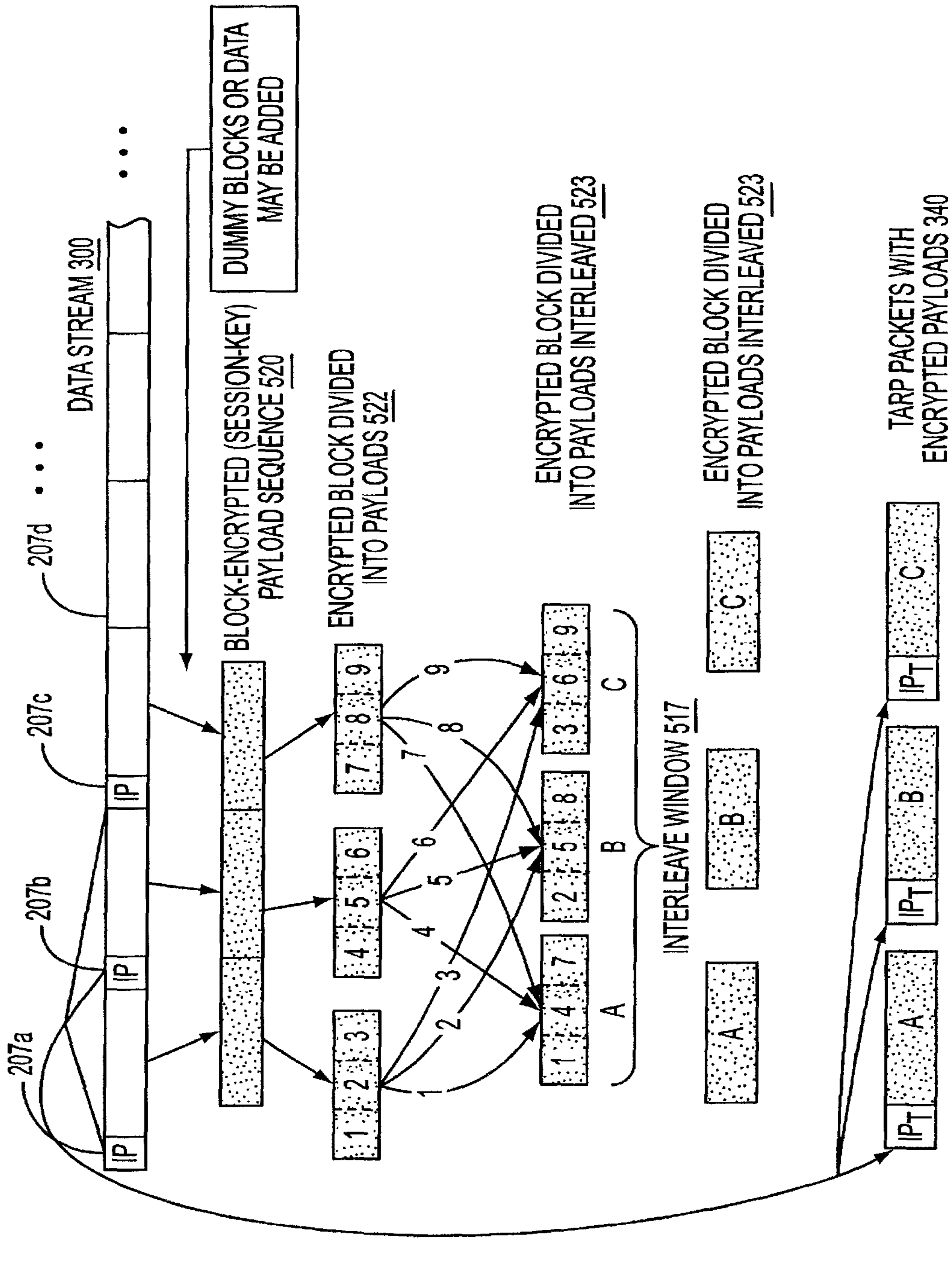

207a
207b
207c
207d
IP
IP
IP
DATA STREAM 300
DUMMY BLOCKS OR DATA MAY BE ADDED
BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE 520
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS 522
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED 523
INTERLEAVE WINDOW 517
A
B
C
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED 523
TARP PACKETS WITH ENCRYPTED PAYLOADS 340
IP_T
IP_T
IP_T

FIG. 3B

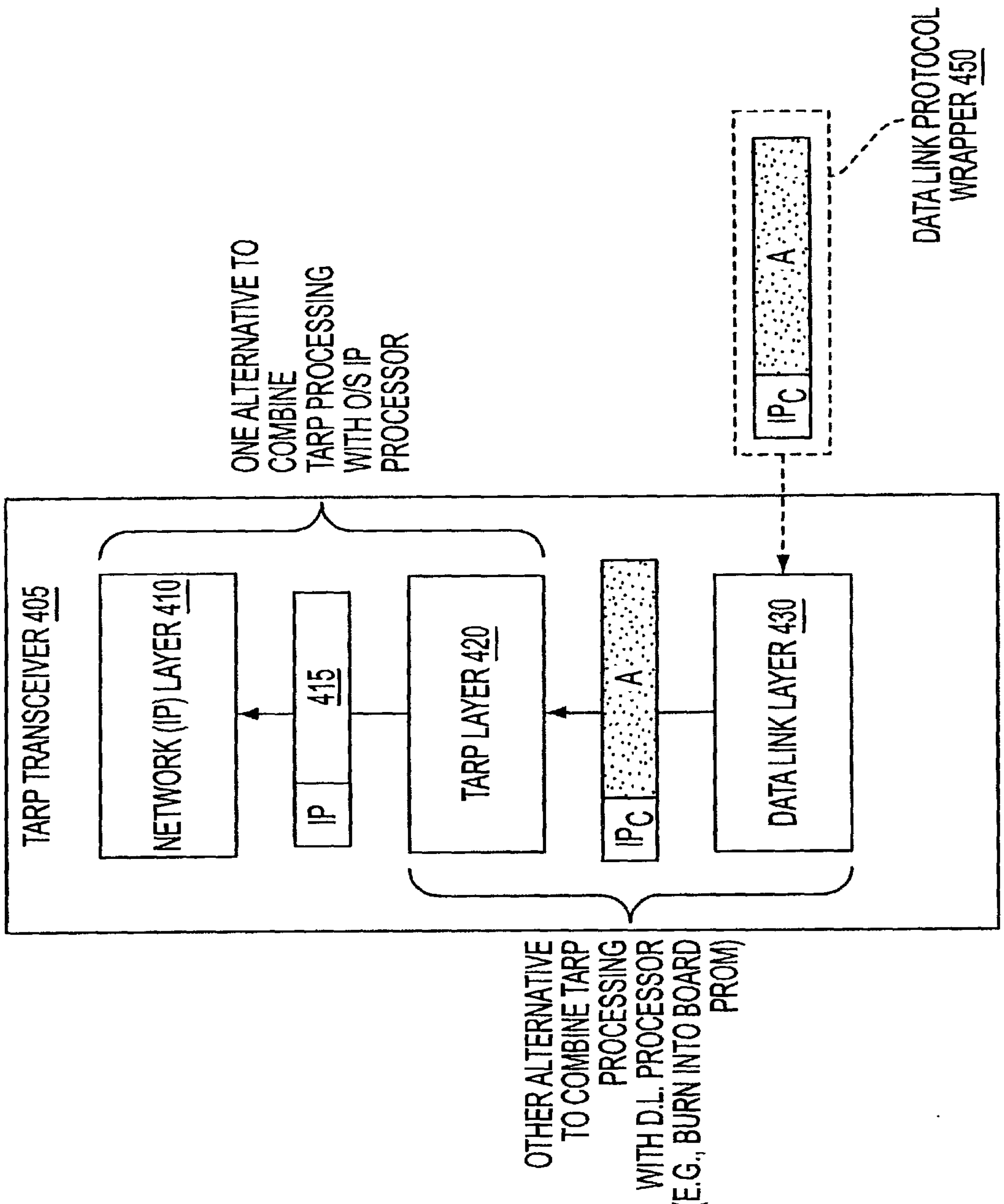

TARP TRANSCEIVER 405
NETWORK (IP) LAYER 410
IP
415
TARP LAYER 420
IPC
A
DATA LINK LAYER 430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (E.G., BURN INTO BOARD PROM)
IPC
A
DATA LINK PROTOCOL WRAPPER 450

FIG. 4

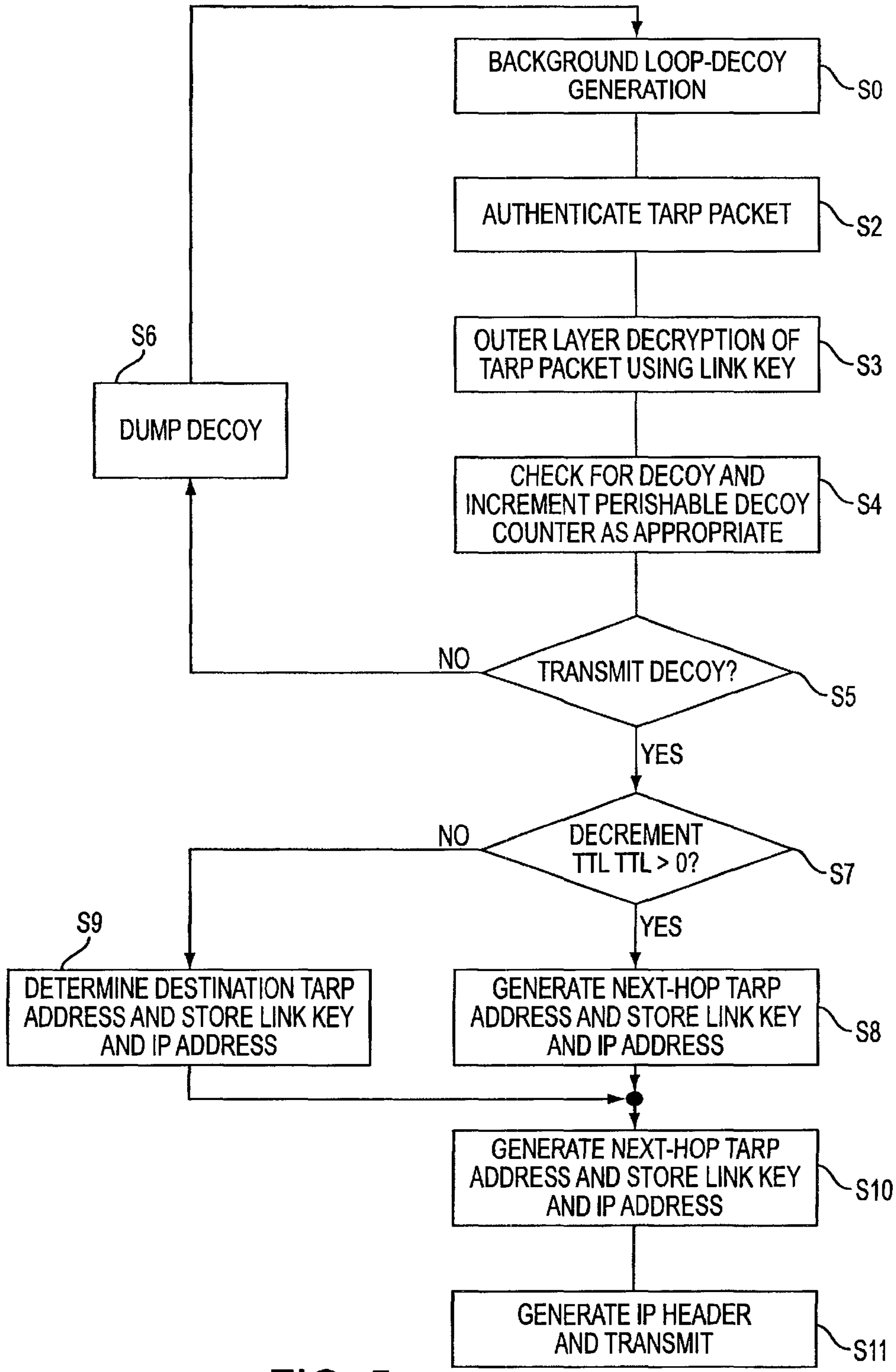

BACKGROUND LOOP-DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
TRANSMIT DECOY?
S5
NO
YES
S6
DUMP DECOY
DECREMENT TTL TTL > 0?
S7
NO
YES
S9
DETERMINE DESTINATION TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S8
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S10
GENERATE IP HEADER AND TRANSMIT
S11

FIG. 5

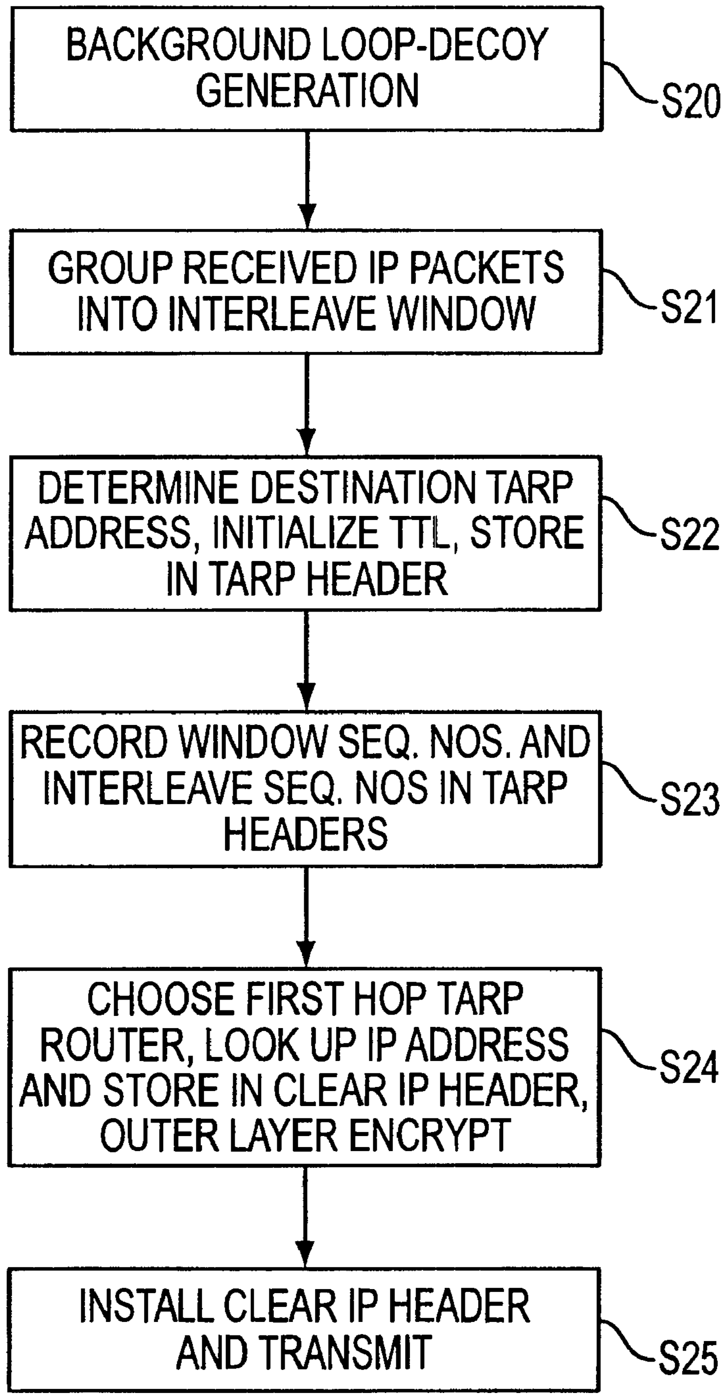

BACKGROUND LOOP-DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR IP HEADER, OUTER LAYER ENCRYPT
S24
INSTALL CLEAR IP HEADER AND TRANSMIT
S25

FIG. 6

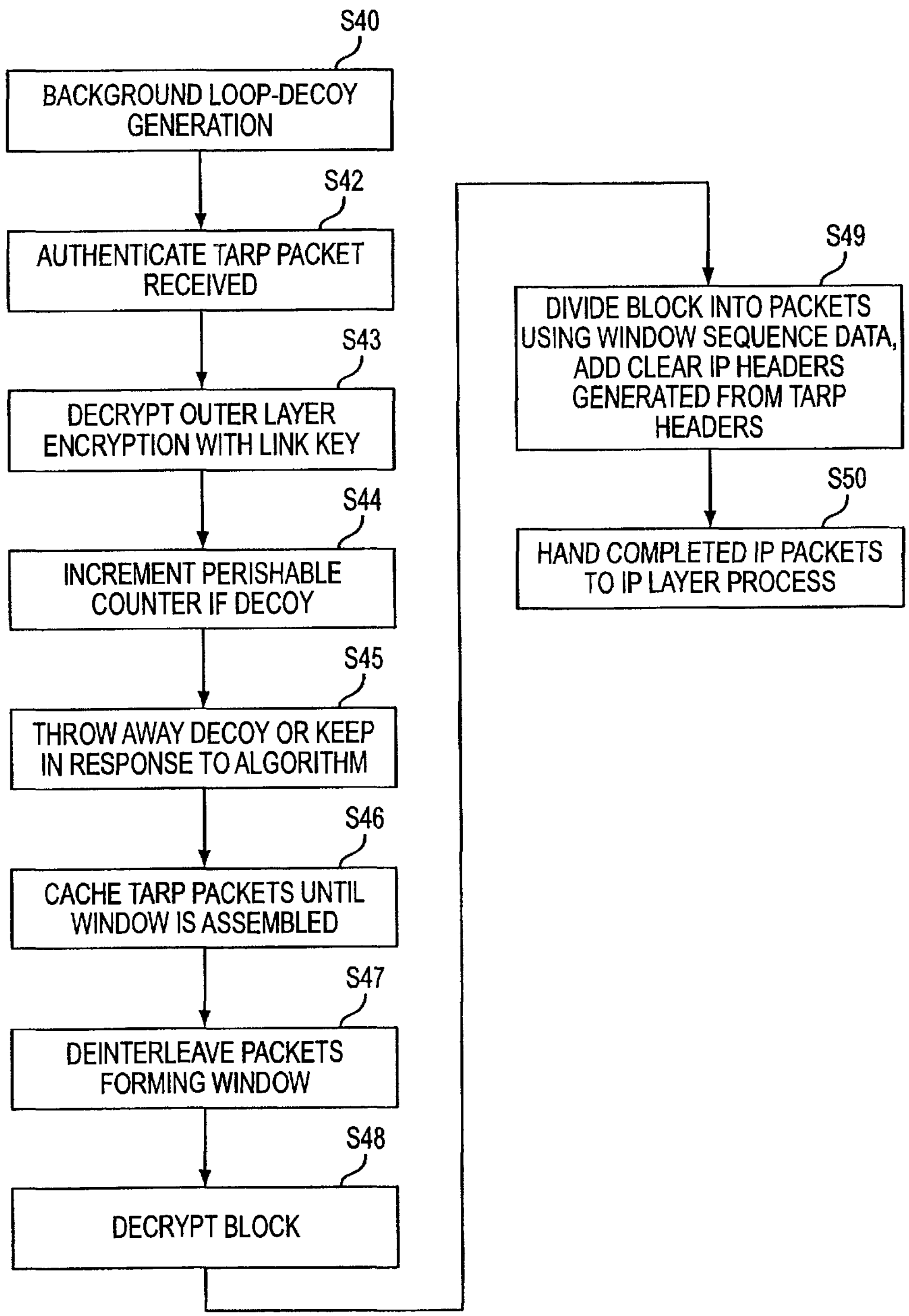

S40
BACKGROUND LOOP-DECOY GENERATION
S42
AUTHENTICATE TARP PACKET RECEIVED
S43
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S44
INCREMENT PERISHABLE COUNTER IF DECOY
S45
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S46
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S47
DEINTERLEAVE PACKETS FORMING WINDOW
S48
DECRYPT BLOCK
S49
DIVIDE BLOCK INTO PACKETS USING WINDOW SEQUENCE DATA, ADD CLEAR IP HEADERS GENERATED FROM TARP HEADERS
S50
HAND COMPLETED IP PACKETS TO IP LAYER PROCESS

FIG. 7

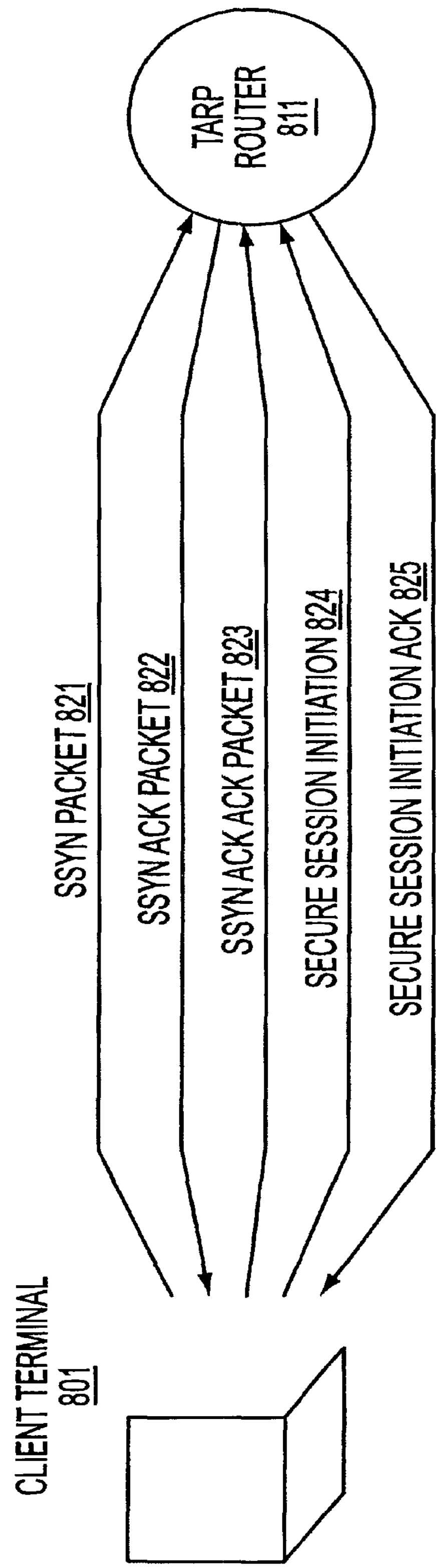
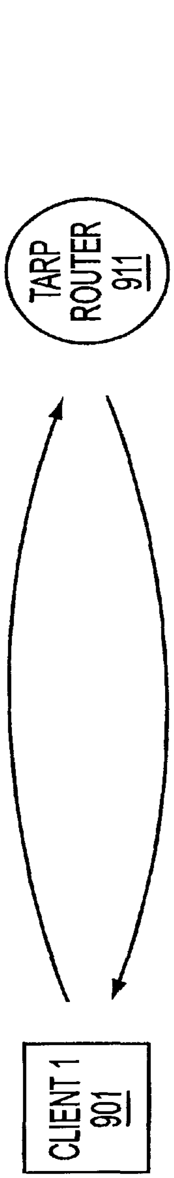

TARP ROUTER 811
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
SECURE SESSION INITIATION 824
SECURE SESSION INITIATION ACK 825
CLIENT TERMINAL 801

FIG. 8



TRANSMIT TABLE 921

131.218.204.98 ,	131.218.204.65
131.218.204.221 ,	131.218.204.97
131.218.204.139 ,	131.218.204.186
131.218.204.12 ,	131.218.204.55
. . .	. . .

RECEIVE TABLE 922

131.218.204.161 ,	131.218.204.89
131.218.204.66 ,	131.218.204.212
131.218.204.201 ,	131.218.204.127
131.218.204.119 ,	131.218.204.49
. . .	. . .

RECEIVE TABLE 924

131.218.204.98 ,	131.218.204.65
131.218.204.221 ,	131.218.204.97
131.218.204.139 ,	131.218.204.186
131.218.204.12 ,	131.218.204.55
. . .	. . .

TRANSMIT TABLE 923

131.218.204.161 ,	131.218.204.89
131.218.204.66 ,	131.218.204.212
131.218.204.201 ,	131.218.204.127
131.218.204.119 ,	131.218.204.49
. . .	. . .

FIG. 9

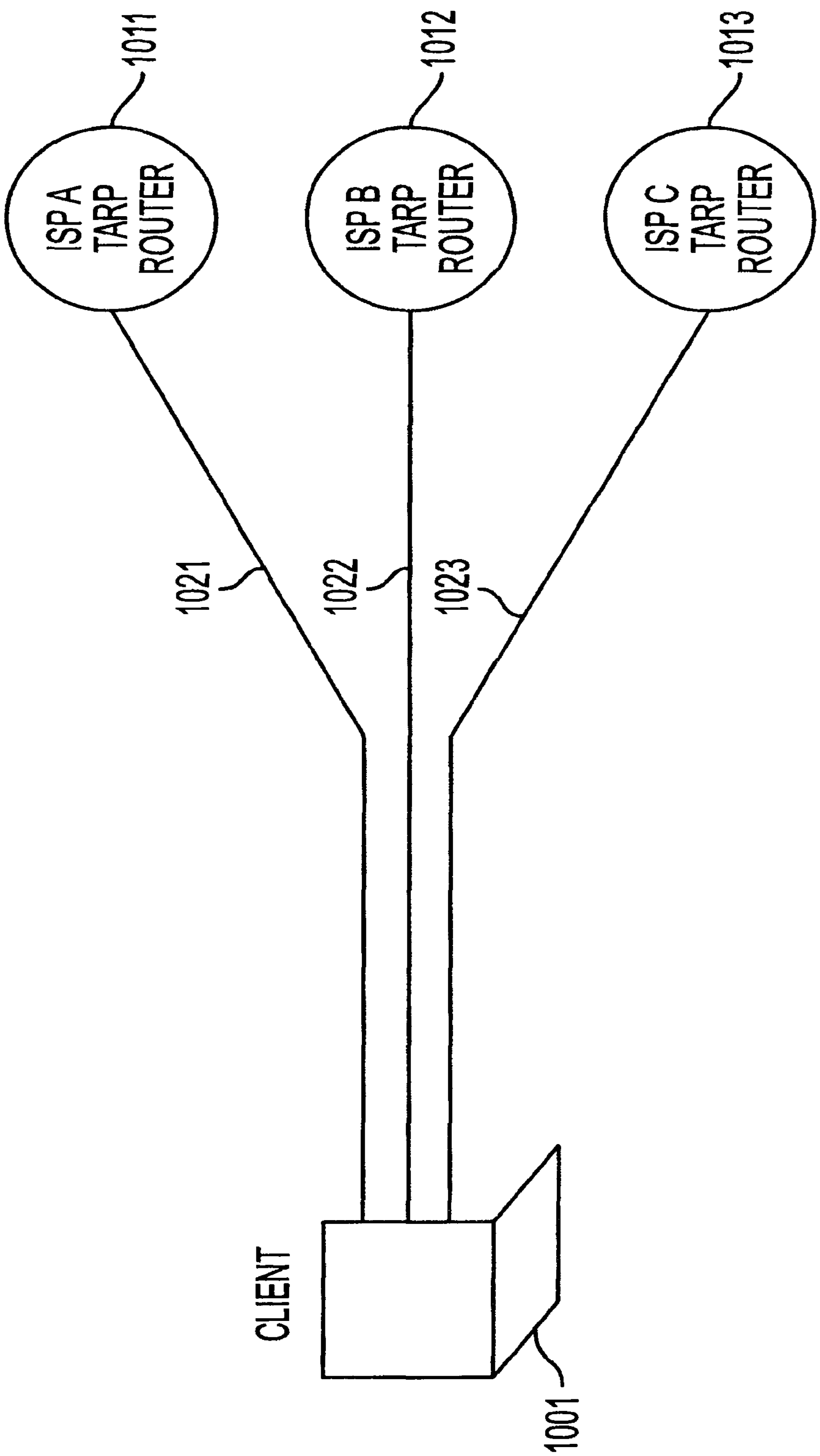
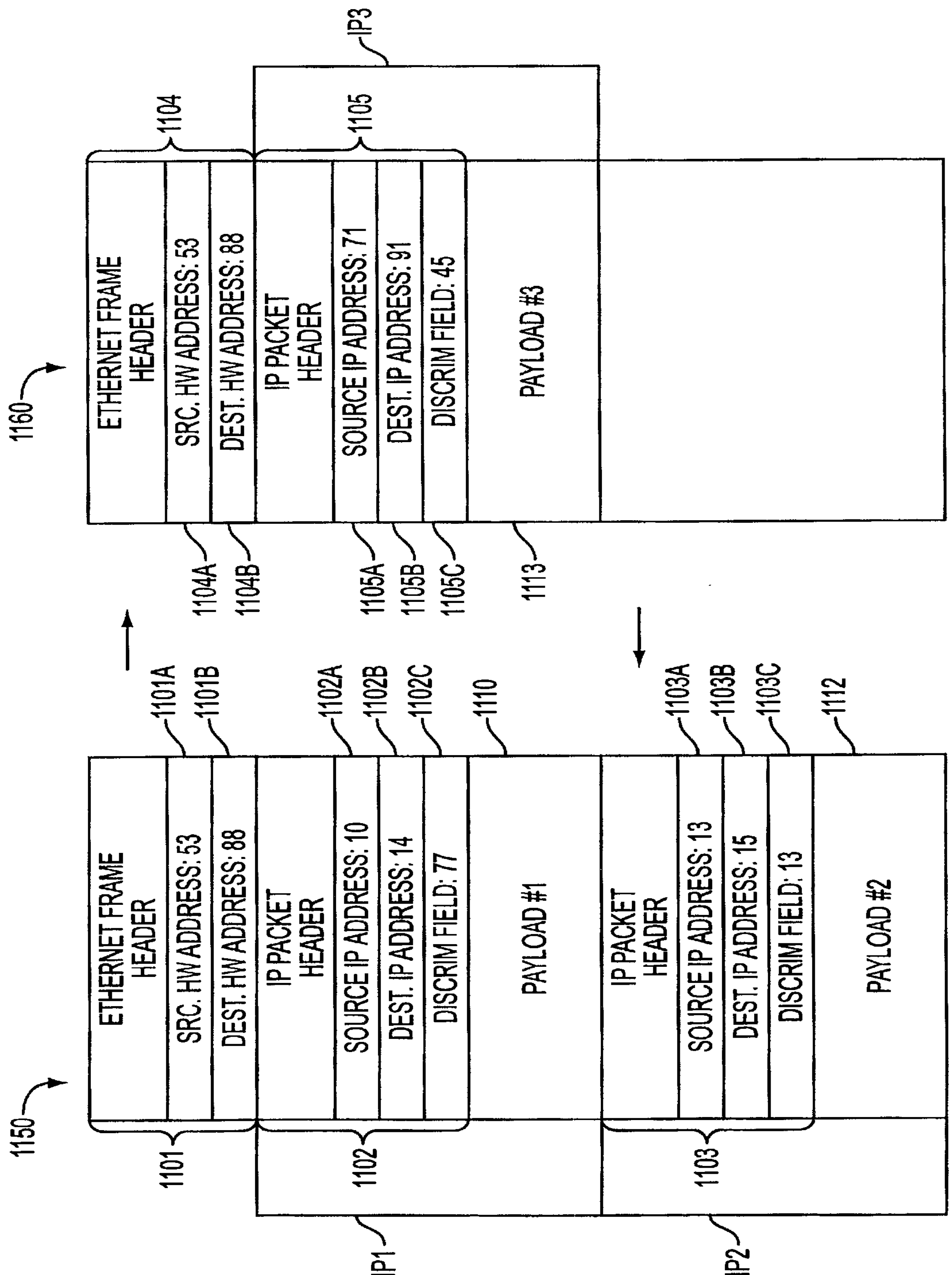

1011
1012
1013
ISP A
TARP
ROUTER
ISP B
TARP
ROUTER
ISP C
TARP
ROUTER
1021
1022
1023
CLIENT
1001

FIG. 10



1160
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 71
DEST. IP ADDRESS: 91
DISCRIM FIELD: 45
PAYLOAD #3
1104
1105
IP3
1104A
1104B
1105A
1105B
1105C
1113
1150
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
1101A
1101B
1102A
1102B
1102C
1110
1103A
1103B
1103C
1112
1101
1102
1103
IP1
IP2

FIG. 11

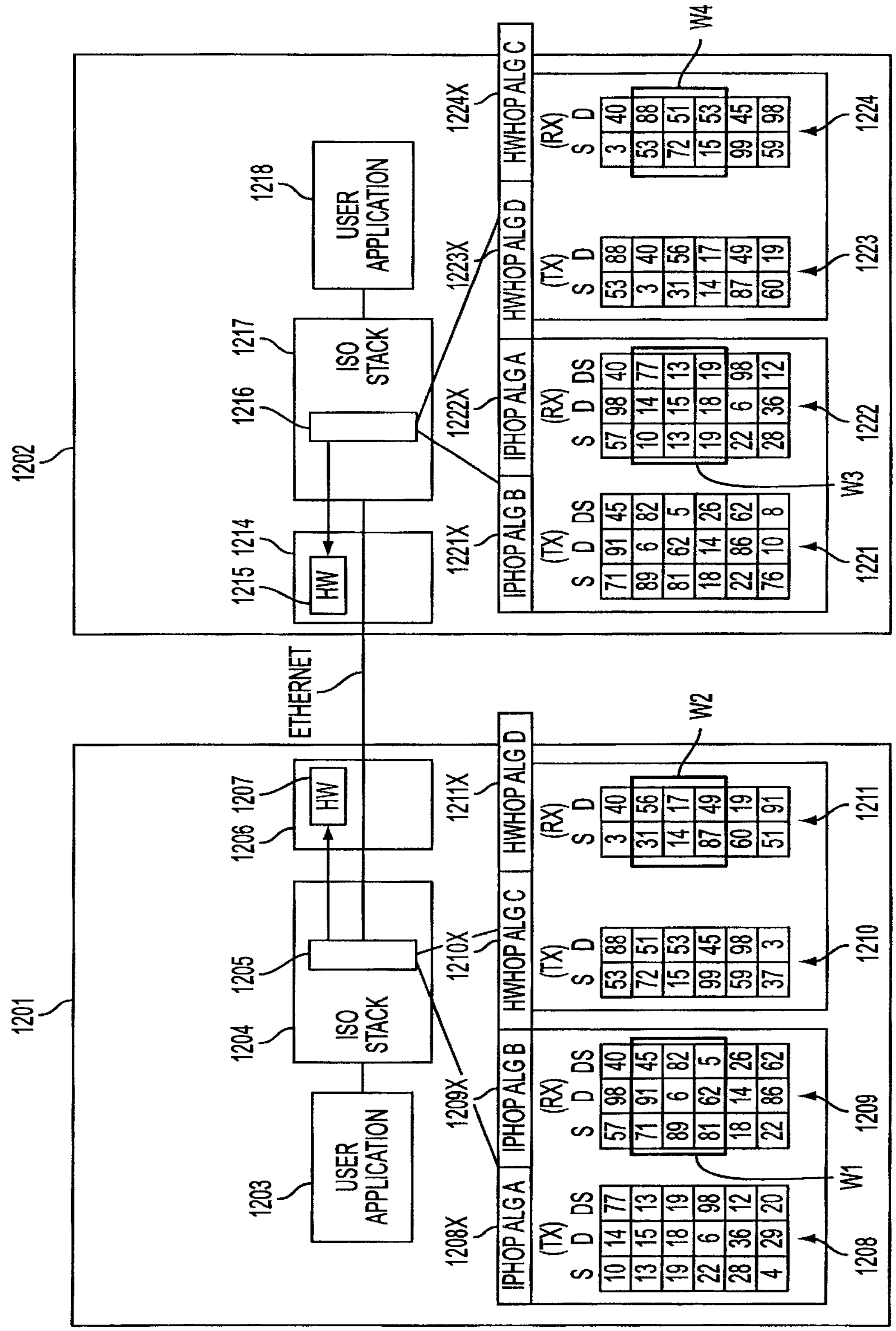

1201
1202
1203
USER APPLICATION
1204
ISO STACK
1205
1206
1207
HW
ETHERNET
1214
1215
HW
1216
1217
ISO STACK
1218
USER APPLICATION
1208X
IPHOP ALG A
1209X
IPHOP ALG B
1210X
HWHOP ALG C
1211X
HWHOP ALG D
1221X
IPHOP ALG B
1222X
IPHOP ALG A
1223X
HWHOP ALG D
1224X
HWHOP ALG C
(TX)
(RX)
S D DS
S D
1208
1209
1210
1211
1221
1222
1223
1224
W1
W2
W3
W4

FIG. 12A

MODE OR EMBODIMENT	HARDWARE ADDRESSES	IP ADDRESSES	DISCRIMINATOR FIELD VALUES
1. PROMISCUOUS	SAME FOR ALL NODES OR COMPLETELY RANDOM	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
2. PROMISCUOUS PER VPN	FIXED FOR EACH VPN	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
3. HARDWARE HOPPING	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC

FIG. 12B

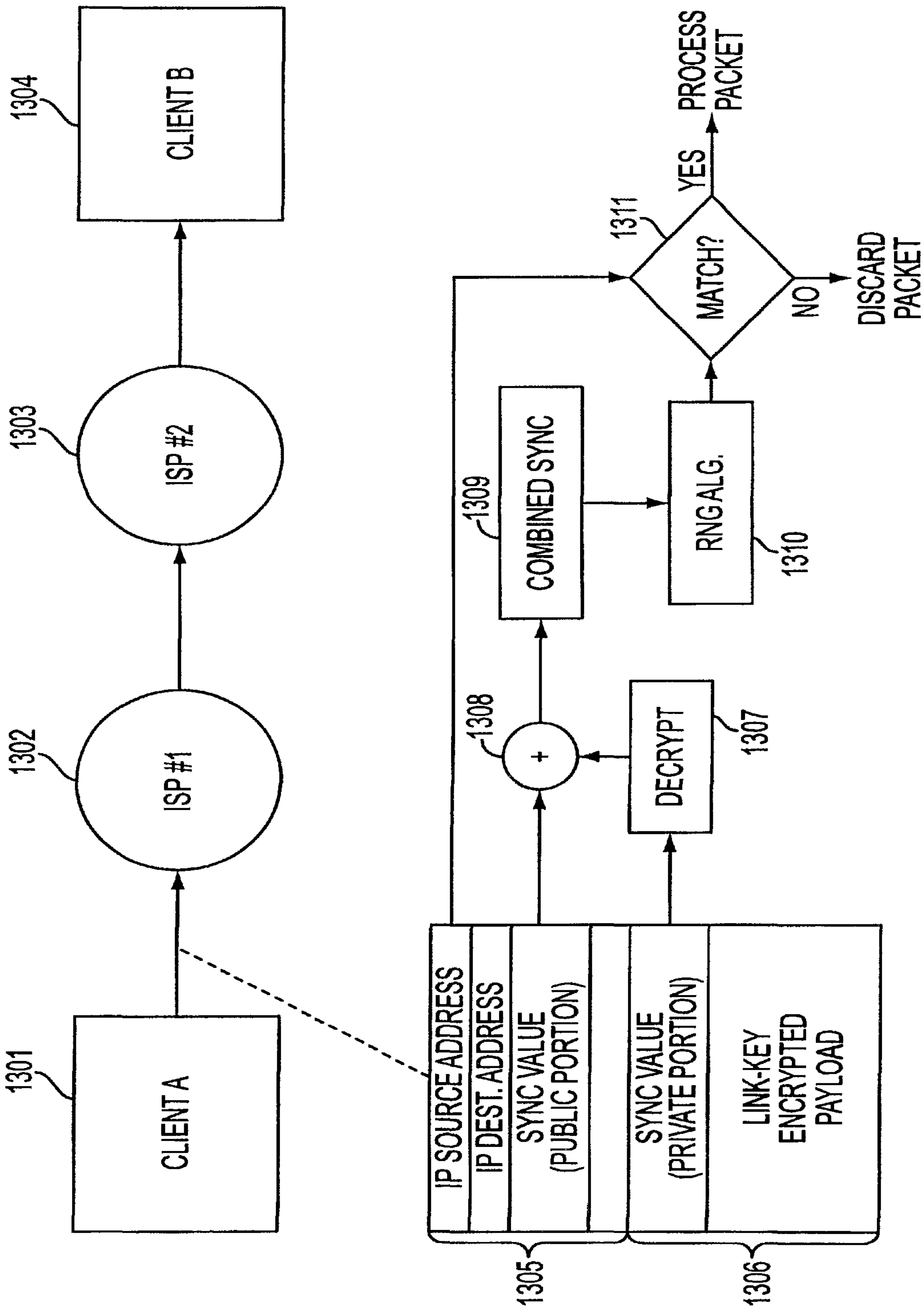

1301
CLIENT A
1302
ISP #1
1303
ISP #2
1304
CLIENT B
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE (PUBLIC PORTION)
SYNC VALUE (PRIVATE PORTION)
LINK-KEY ENCRYPTED PAYLOAD
1305
1306
DECRYPT
1307
+
1308
COMBINED SYNC
1309
RNG ALG.
1310
MATCH?
1311
YES
PROCESS PACKET
NO
DISCARD PACKET

FIG. 13

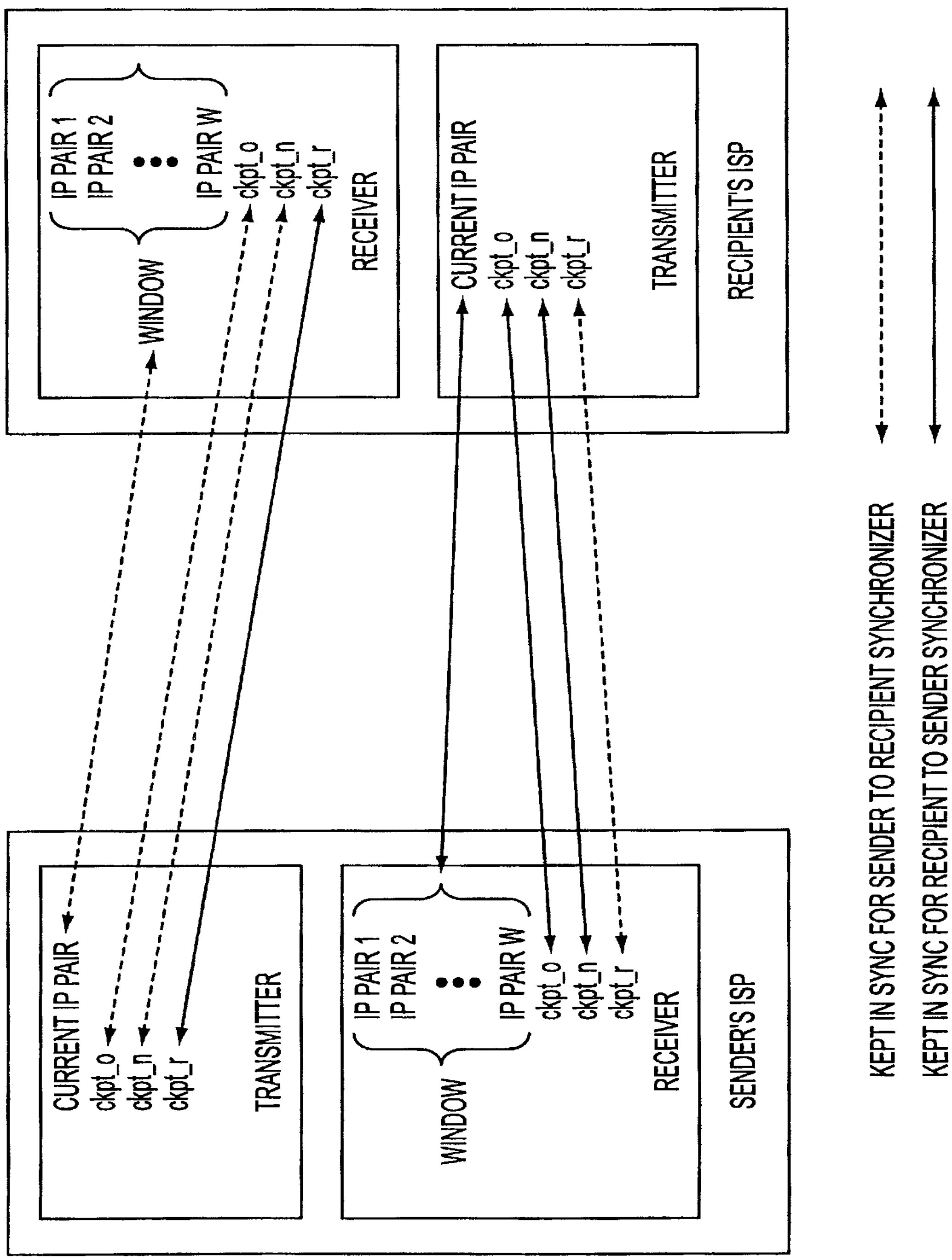

WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
SENDER'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER
KEPT IN SYNC FOR RECIPIENT TO SENDER SYNCHRONIZER

FIG. 14

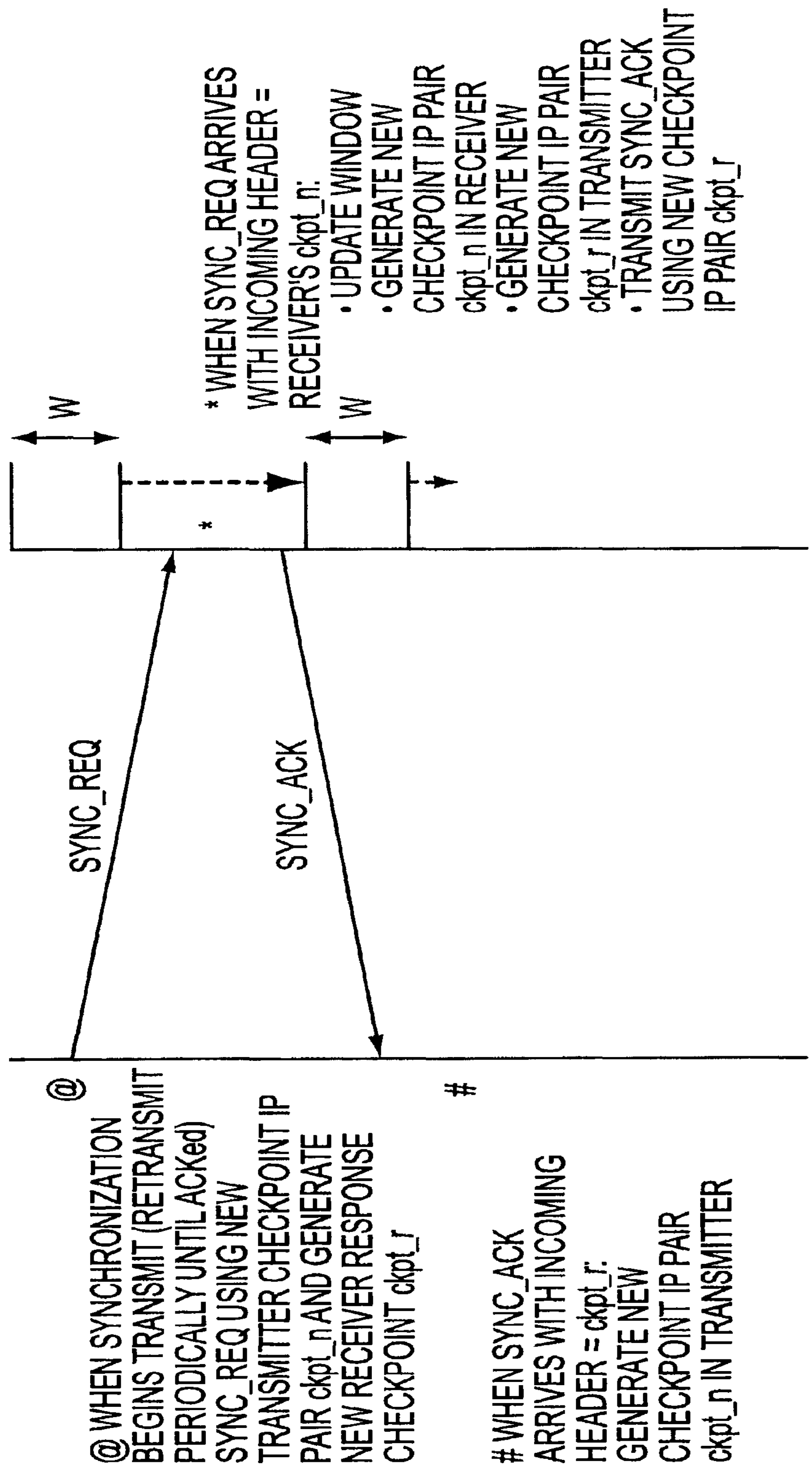

W
W
SYNC_REQ
SYNC_ACK
@
#
*
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
# WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r: GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN TRANSMITTER
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
• UPDATE WINDOW
• GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN RECEIVER
• GENERATE NEW CHECKPOINT IP PAIR ckpt_r IN TRANSMITTER
• TRANSMIT SYNC_ACK USING NEW CHECKPOINT IP PAIR ckpt_r

FIG. 15

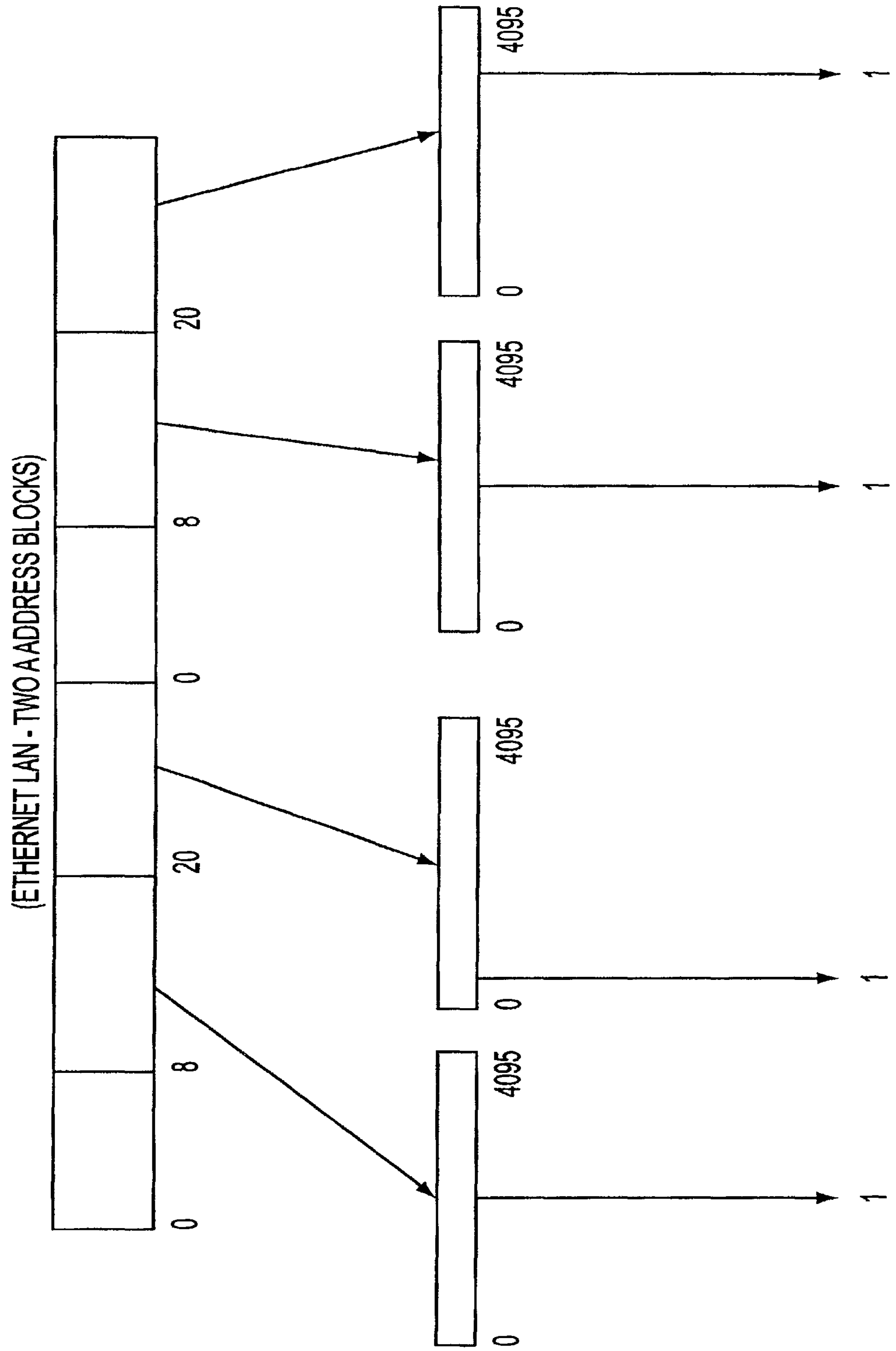

(ETHERNET LAN - TWO A ADDRESS BLOCKS)
0
8
20
0
8
20
0
4095
0
4095
0
4095
0
4095
1
1
1
1

FIG. 16

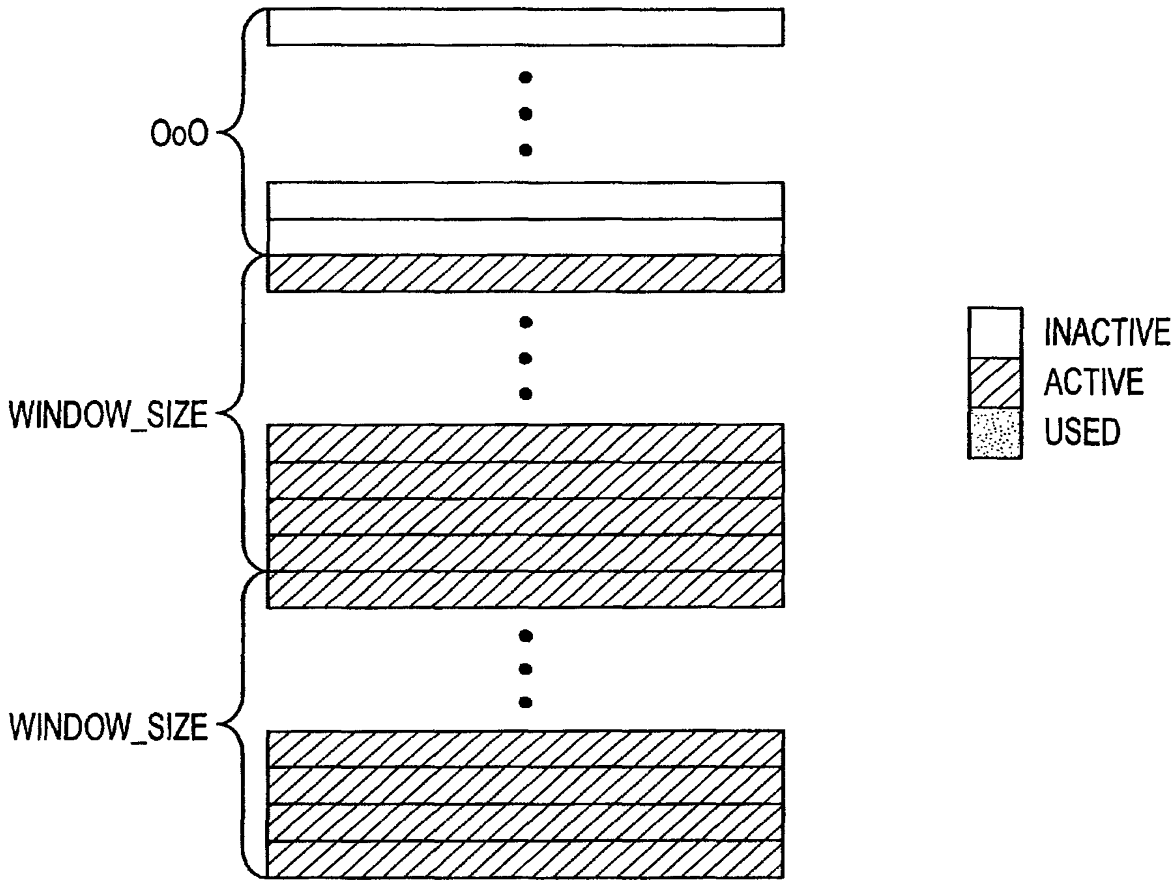


FIG. 17

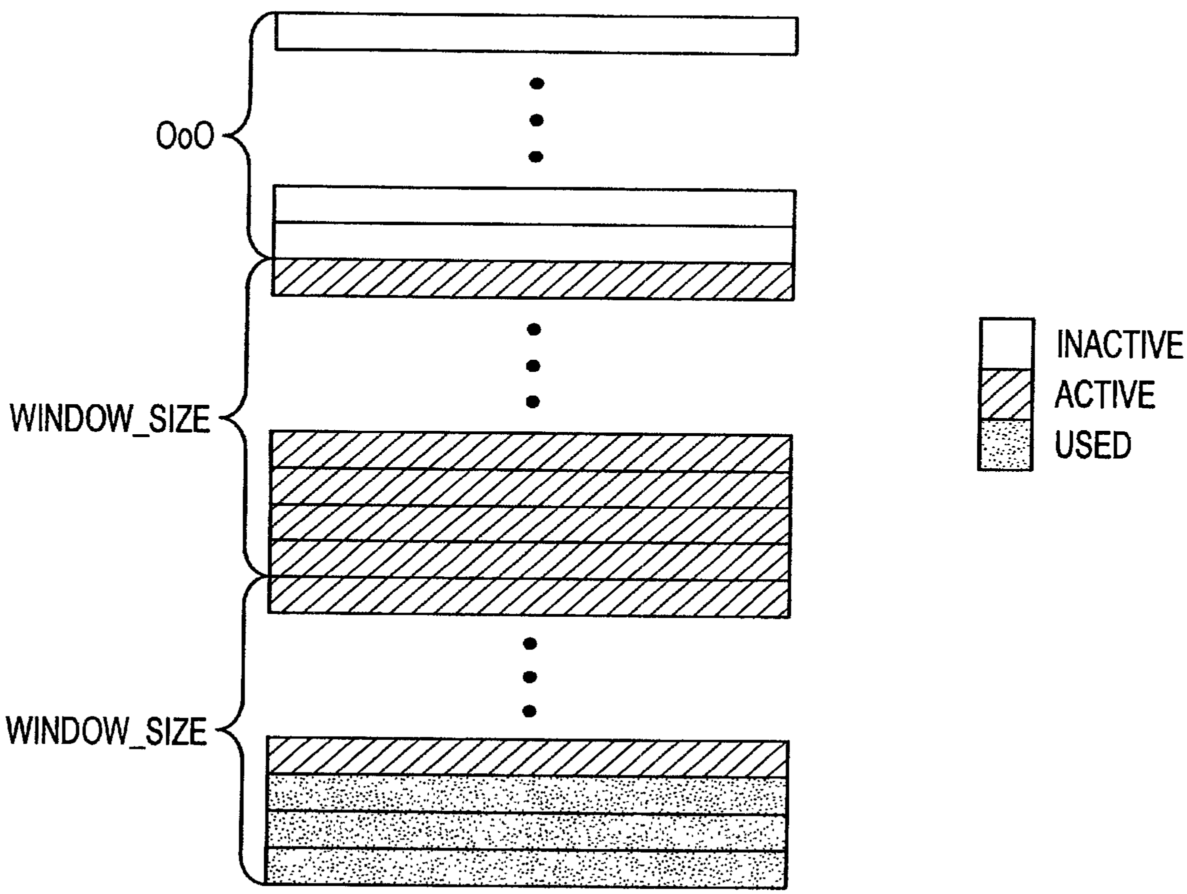


FIG. 18

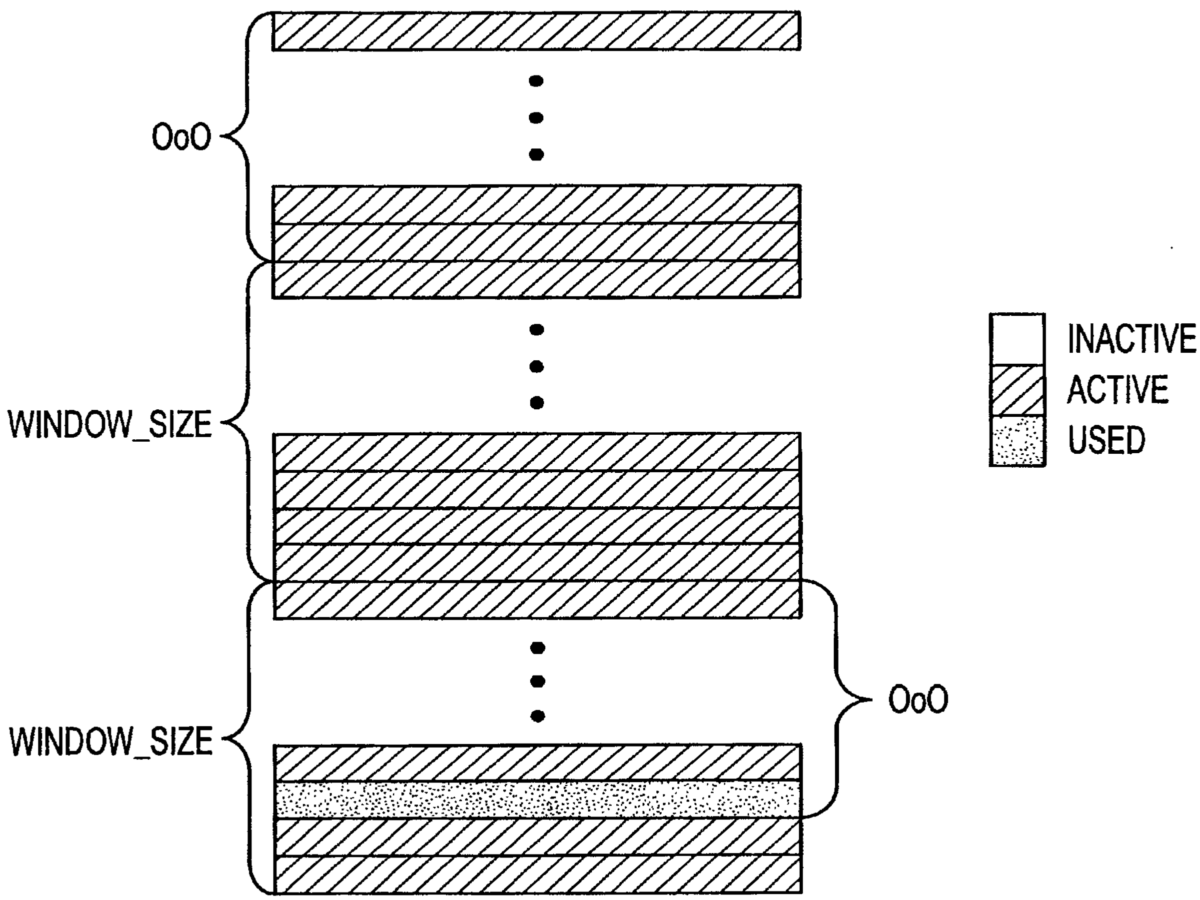


FIG. 19

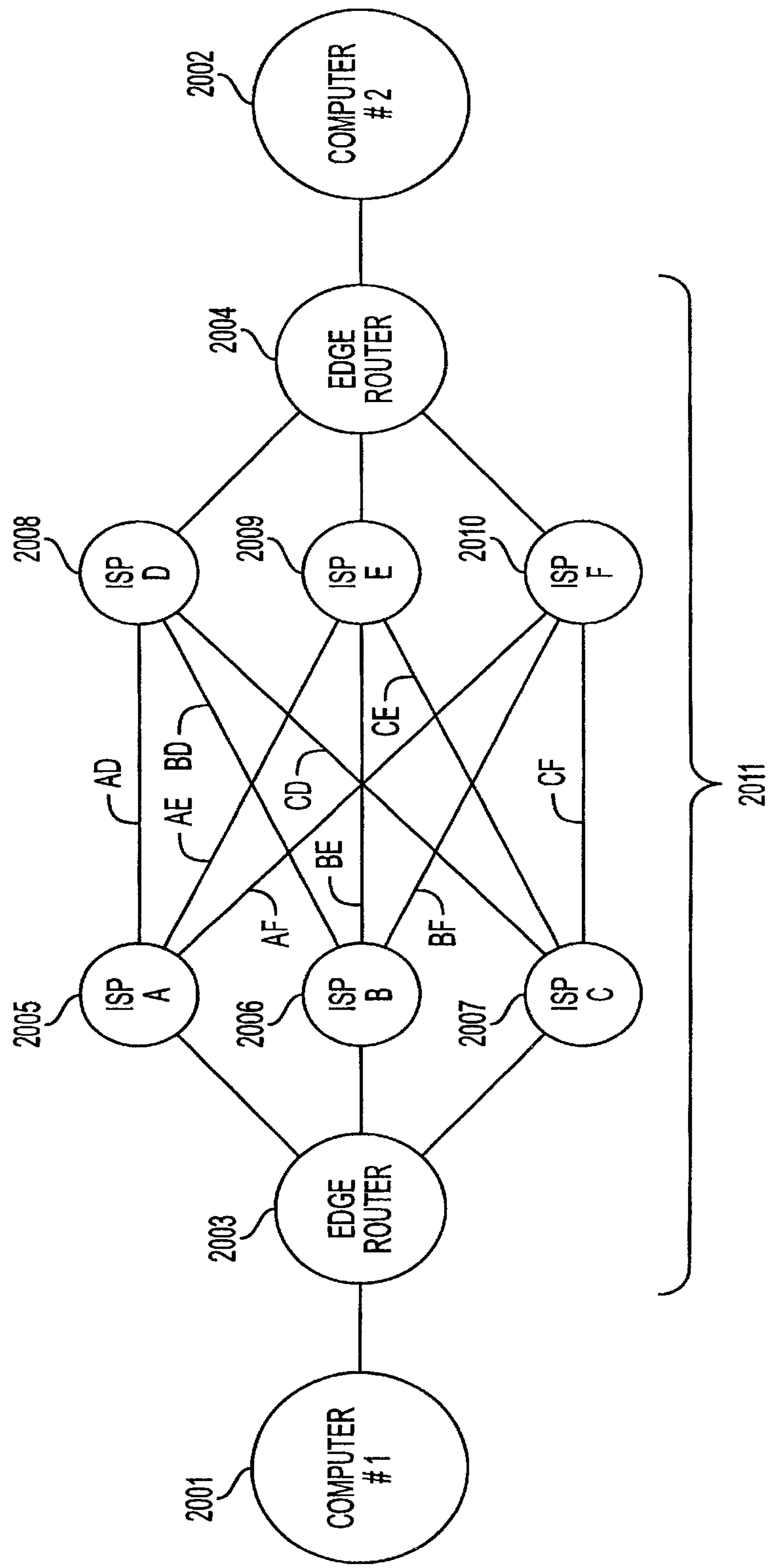

COMPUTER #2
2002
EDGE ROUTER
2004
ISP D
2008
ISP E
2009
ISP F
2010
AD
AE
BD
CD
CE
BE
AF
BF
CF
ISP A
2005
ISP B
2006
ISP C
2007
EDGE ROUTER
2003
COMPUTER #1
2001
2011

FIG. 20

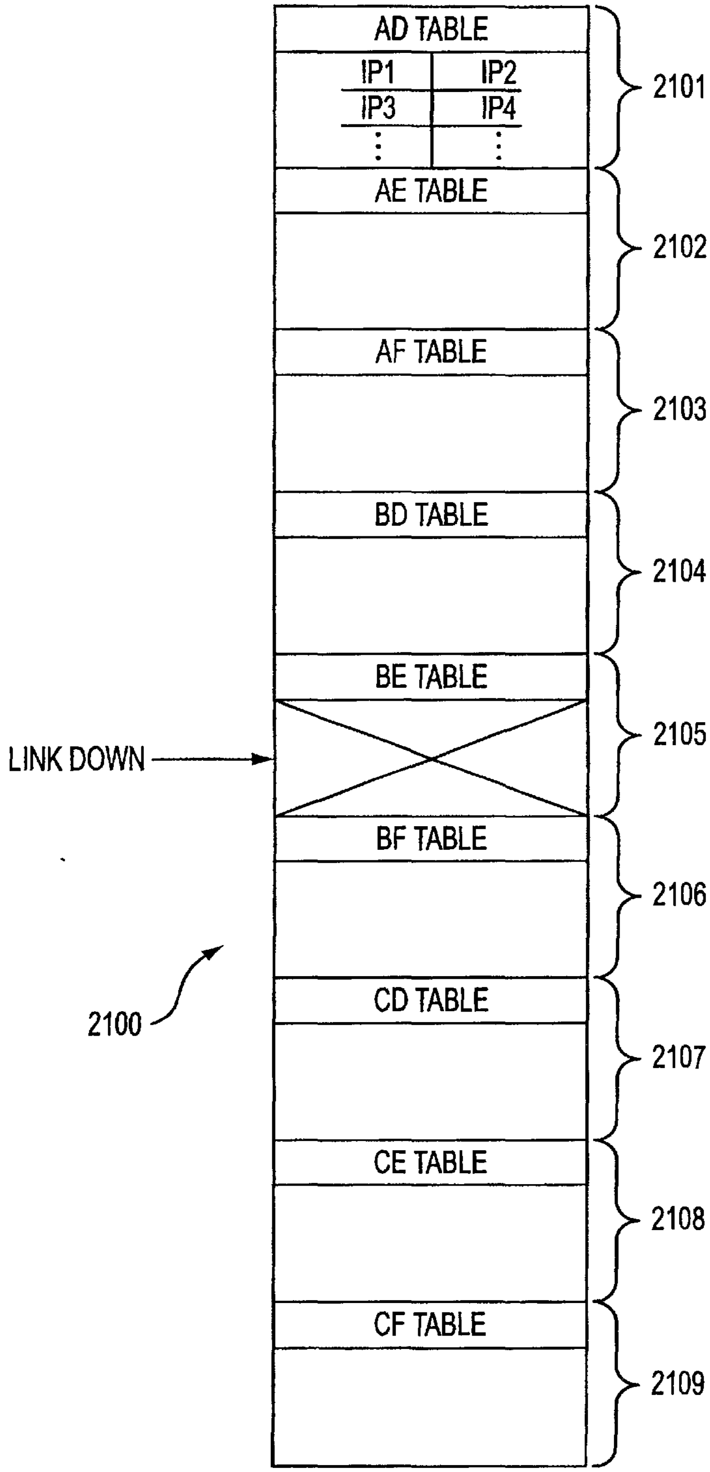

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
2105
LINK DOWN
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

FIG. 21

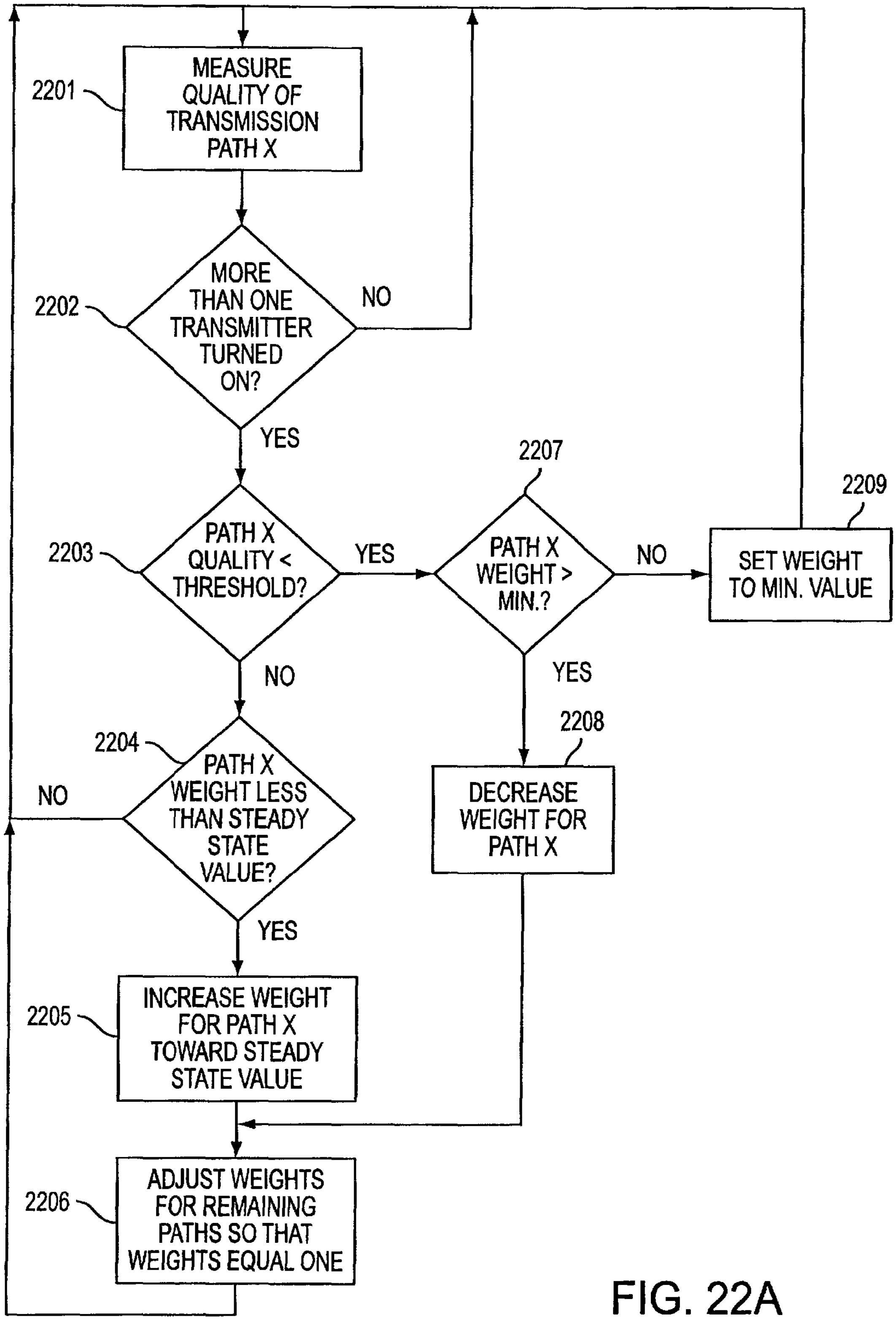

MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
2202
NO
YES
PATH X QUALITY < THRESHOLD?
2203
YES
PATH X WEIGHT > MIN.?
2207
NO
SET WEIGHT TO MIN. VALUE
2209
NO
YES
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
2204
NO
DECREASE WEIGHT FOR PATH X
2208
YES
INCREASE WEIGHT FOR PATH X TOWARD STEADY STATE VALUE
2205
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2206

FIG. 22A

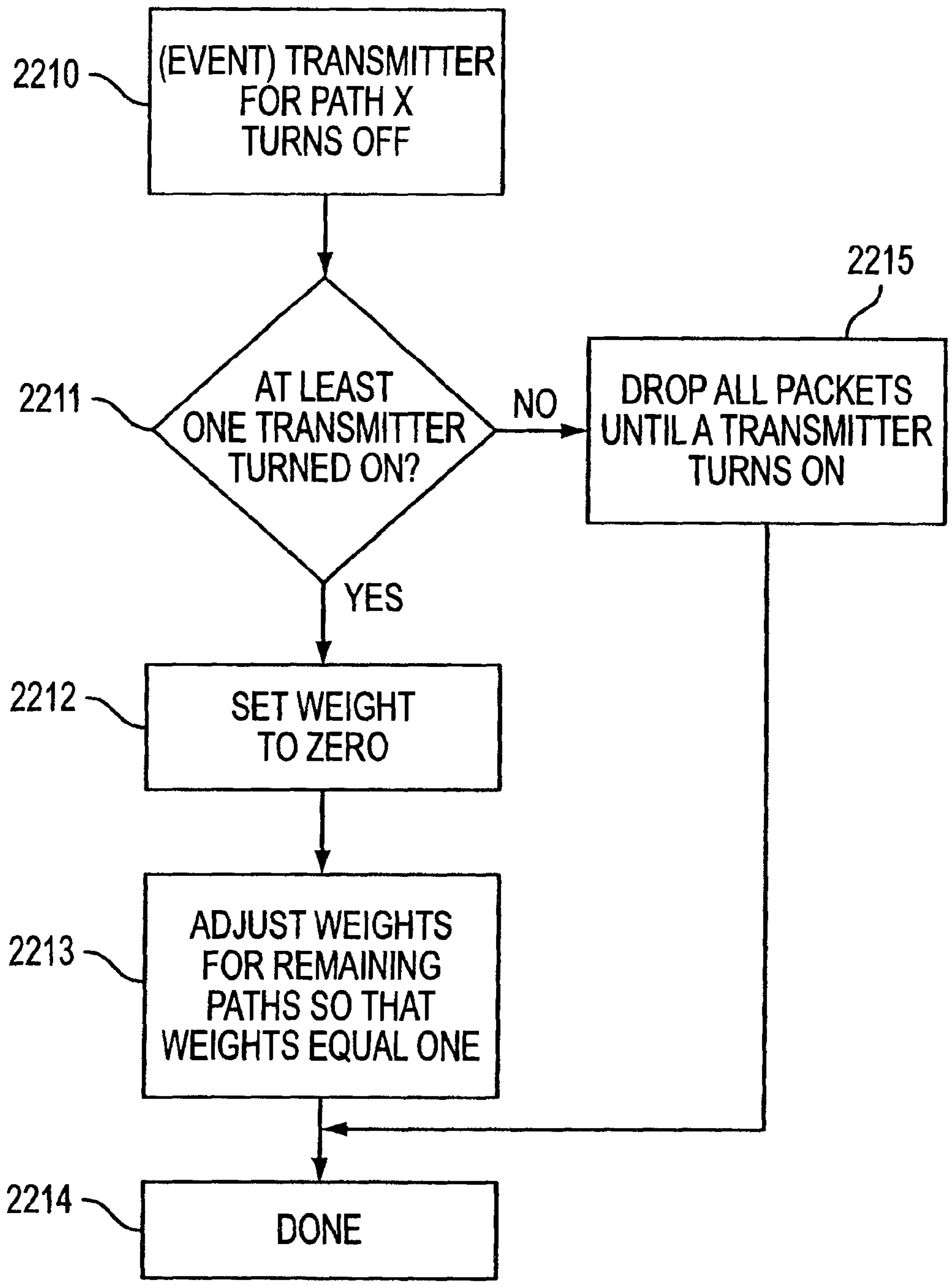

2210
(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2211
AT LEAST ONE TRANSMITTER TURNED ON?
NO
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
YES
2212
SET WEIGHT TO ZERO
2213
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2214
DONE

FIG. 22B

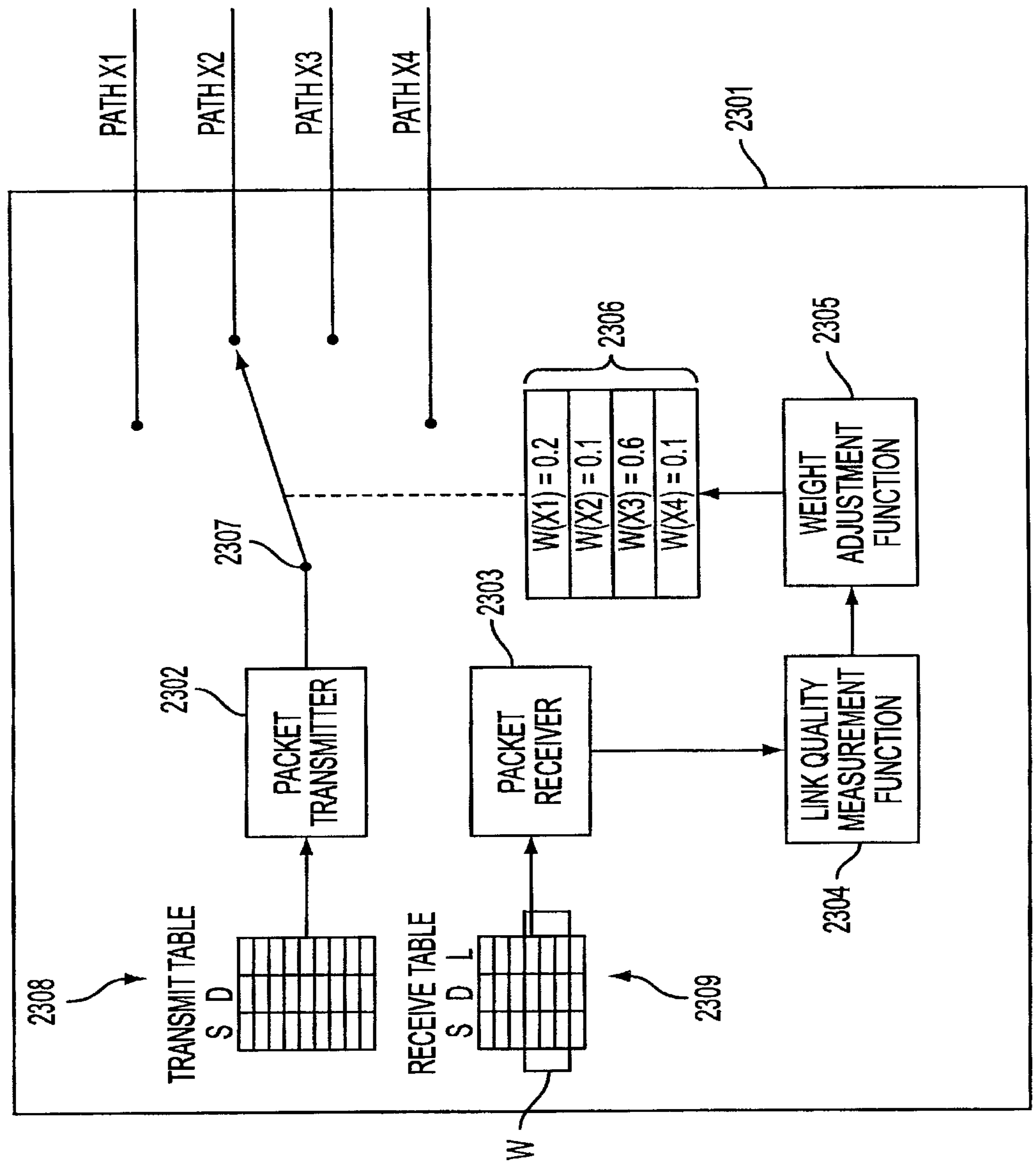

PATH X1
PATH X2
PATH X3
PATH X4
2301
2306
2305
W(X1) = 0.2
W(X2) = 0.1
W(X3) = 0.6
W(X4) = 0.1
WEIGHT ADJUSTMENT FUNCTION
2307
2303
2302
PACKET TRANSMITTER
PACKET RECEIVER
LINK QUALITY MEASUREMENT FUNCTION
2304
2308
TRANSMIT TABLE
S D
RECEIVE TABLE
S D L
2309
W

FIG. 23

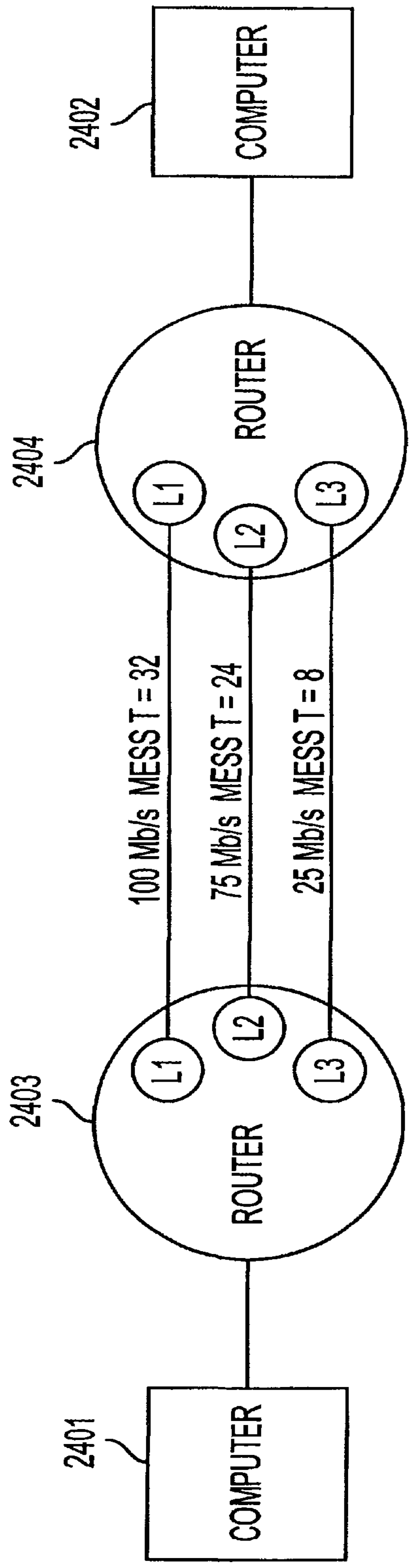

COMPUTER
2401
ROUTER
2403
L1
L2
L3
100 Mb/s MESS T = 32
75 Mb/s MESS T = 24
25 Mb/s MESS T = 8
ROUTER
2404
L1
L2
L3
COMPUTER
2402

FIG. 24

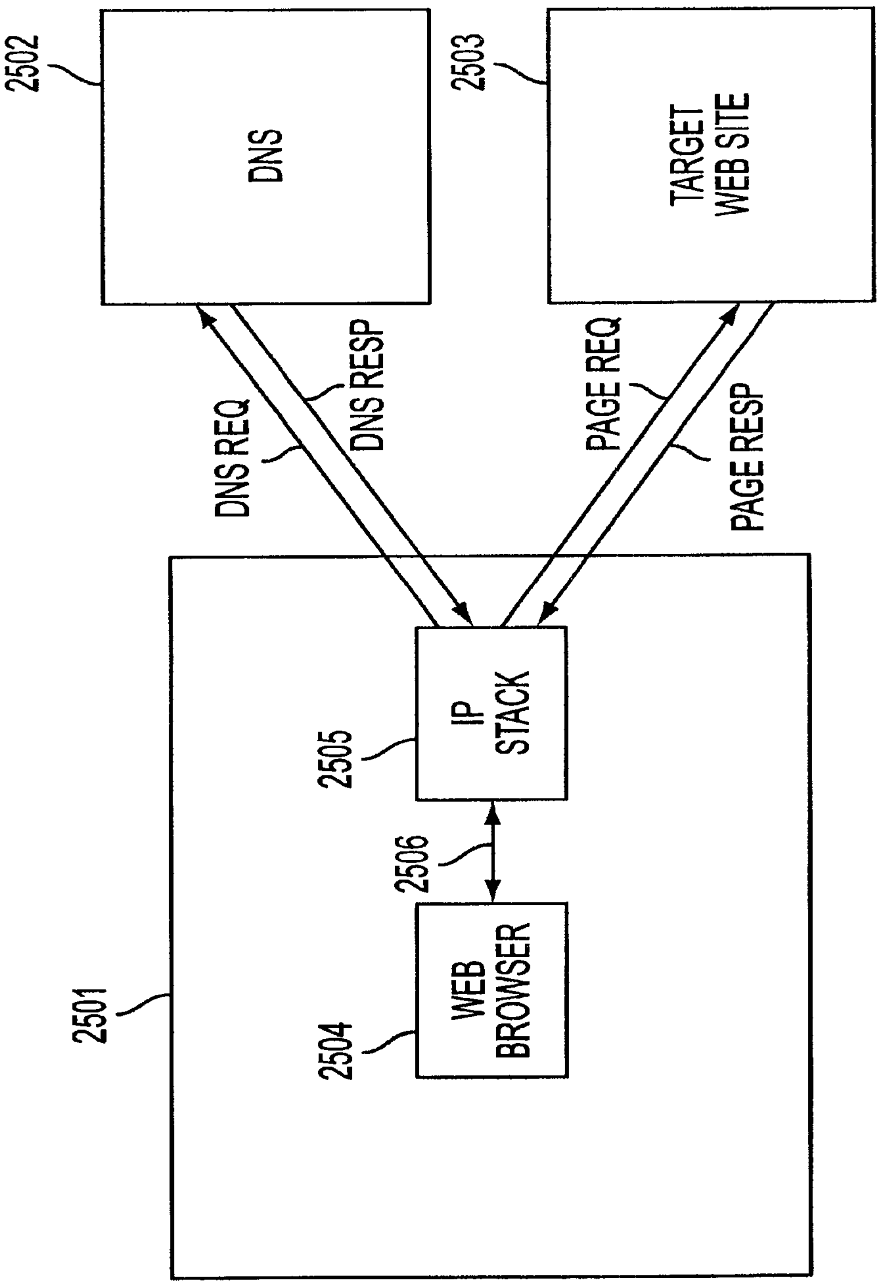


FIG. 25
(PRIOR ART)

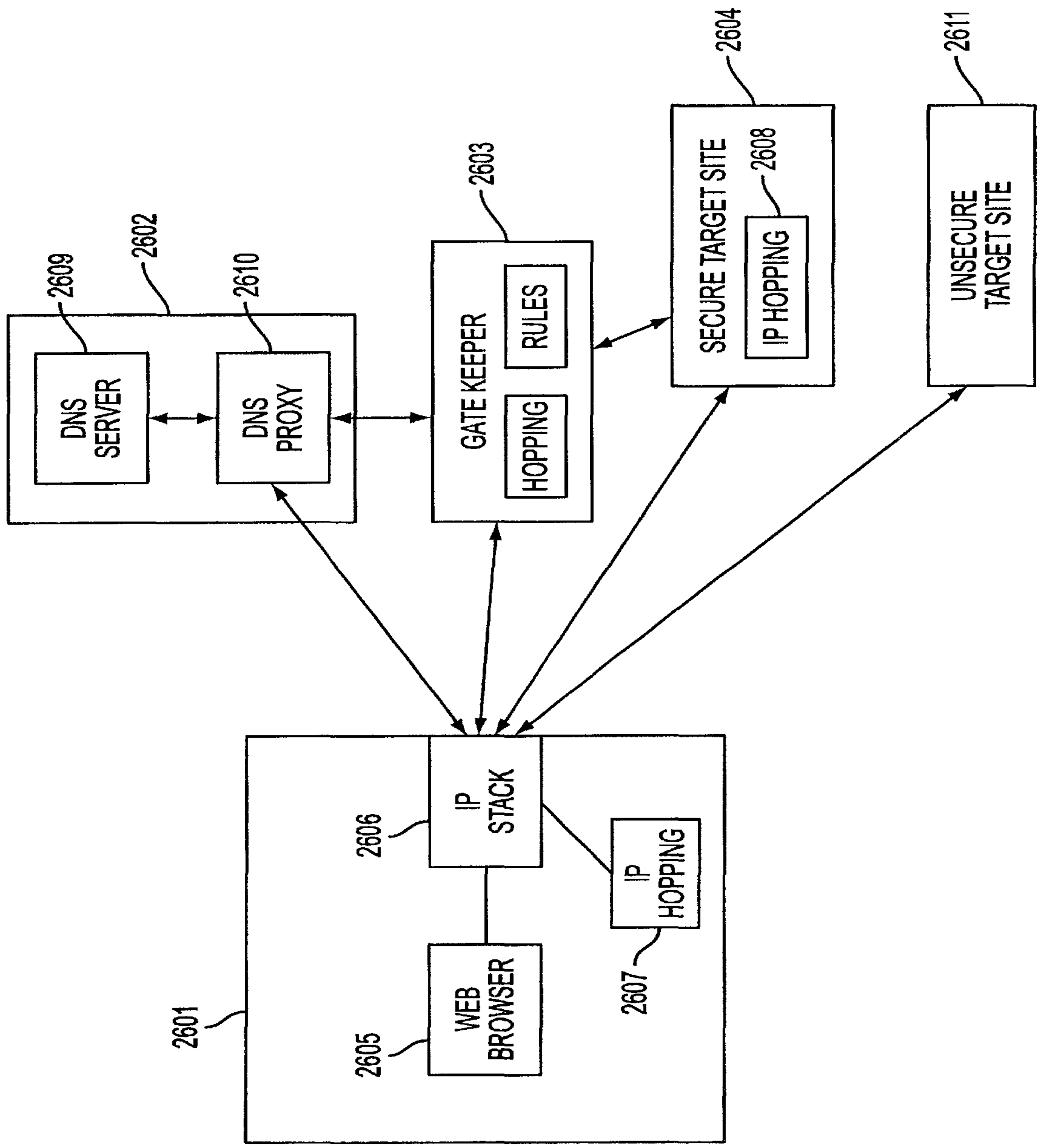

2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
DNS SERVER
DNS PROXY
GATE KEEPER
HOPPING
RULES
SECURE TARGET SITE
IP HOPPING
UNSECURE TARGET SITE
WEB BROWSER
IP STACK
IP HOPPING

FIG. 26

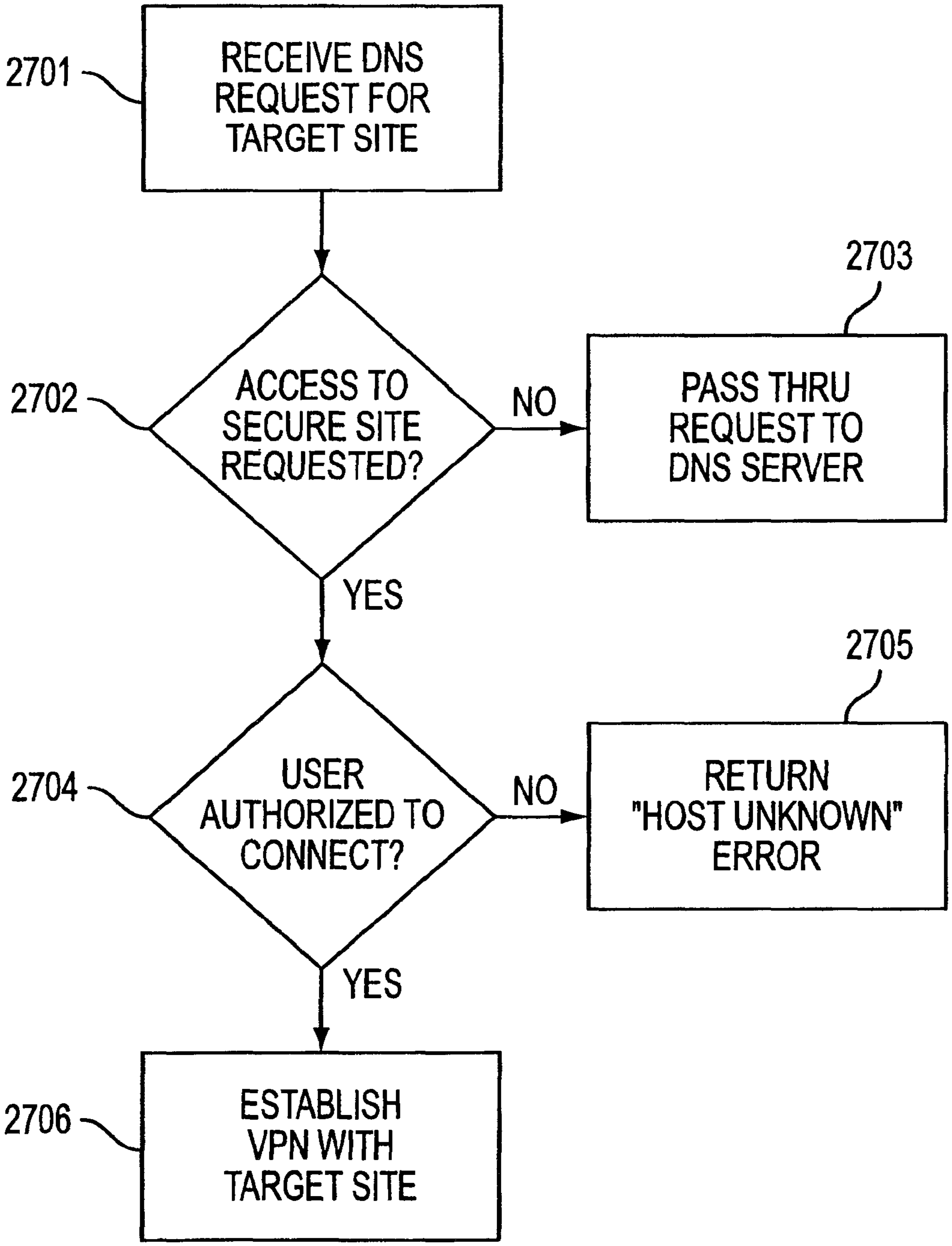
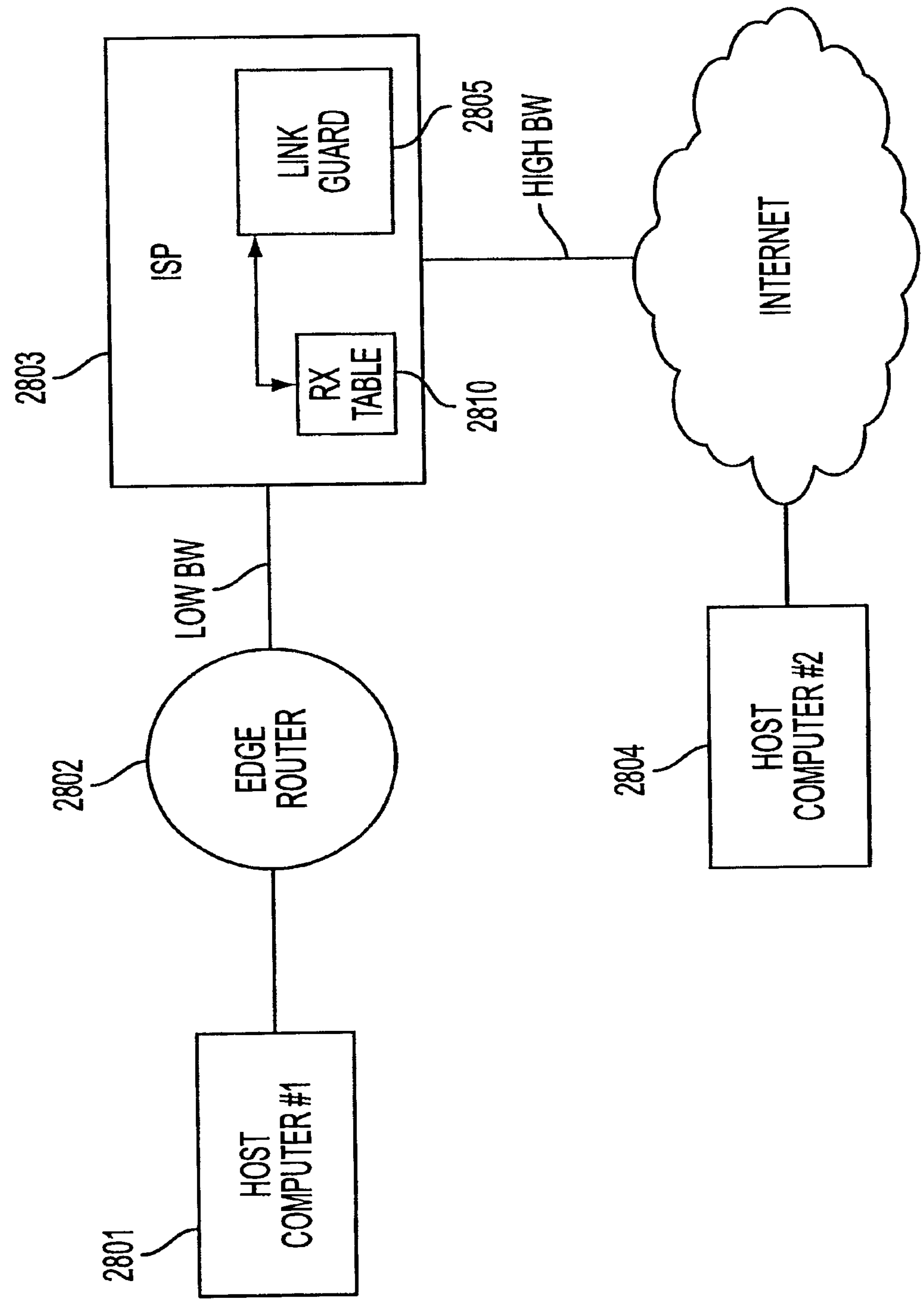

2701
RECEIVE DNS REQUEST FOR TARGET SITE
2702
ACCESS TO SECURE SITE REQUESTED?
NO
2703
PASS THRU REQUEST TO DNS SERVER
YES
2704
USER AUTHORIZED TO CONNECT?
NO
2705
RETURN "HOST UNKNOWN" ERROR
YES
2706
ESTABLISH VPN WITH TARGET SITE

FIG. 27



2803
ISP
LINK GUARD
2805
RX TABLE
2810
HIGH BW
INTERNET
LOW BW
2802
EDGE ROUTER
2804
HOST COMPUTER #2
2801
HOST COMPUTER #1

FIG. 28

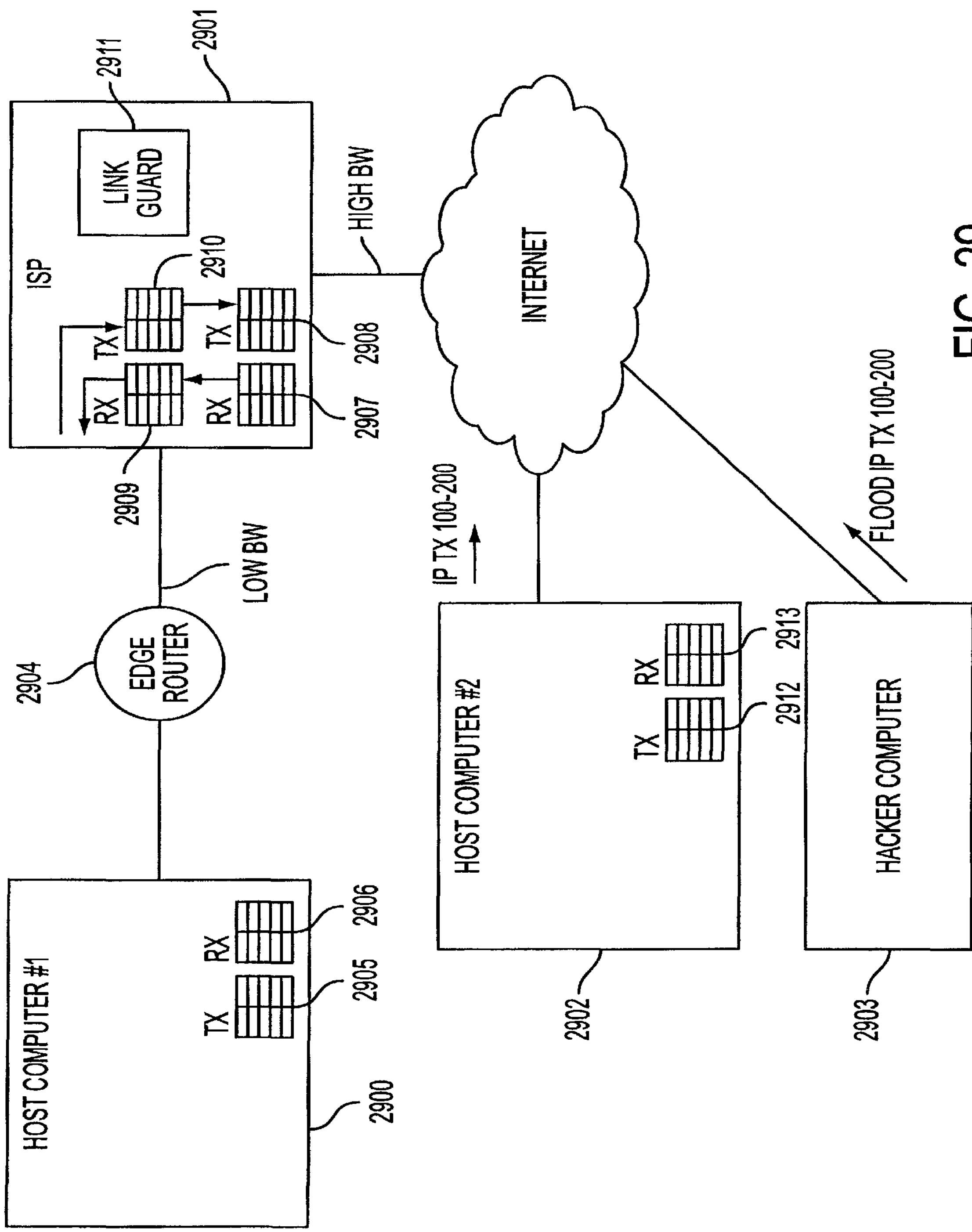

2911
2901
LINK GUARD
ISP
2910
HIGH BW
TX
TX
RX
RX
2908
2907
2909
INTERNET
LOW BW
IP TX 100-200
FLOOD IP TX 100-200
2904
EDGE ROUTER
HOST COMPUTER #2
RX
TX
2913
2912
HACKER COMPUTER
HOST COMPUTER #1
RX
TX
2906
2905
2900
2902
2903

FIG. 29

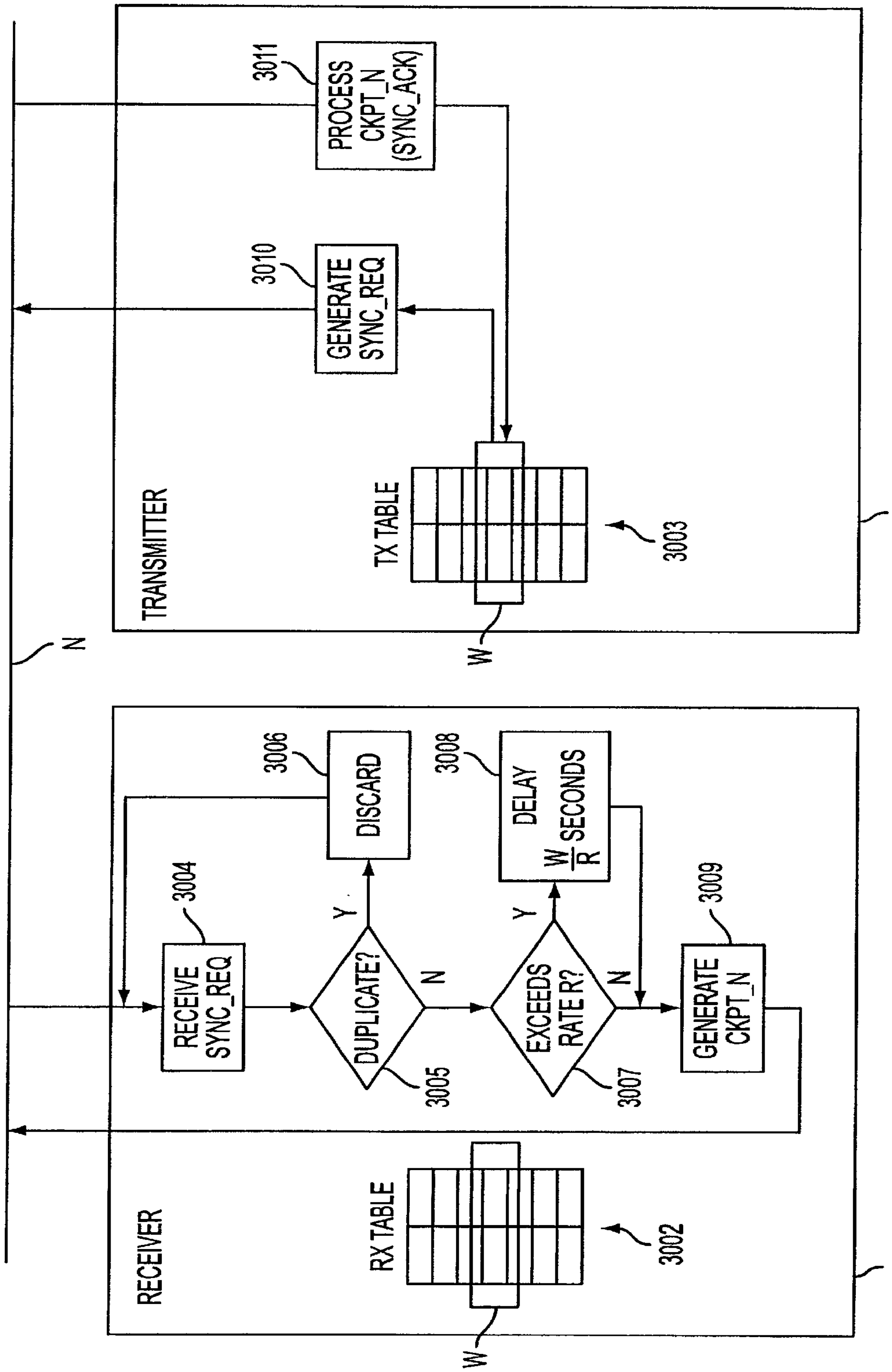

TRANSMITTER
PROCESS CKPT_N (SYNC_ACK)
3011
GENERATE SYNC_REQ
3010
TX TABLE
3003
3001
W
N
RECEIVER
RECEIVE SYNC_REQ
3004
DUPLICATE?
3005
Y
N
DISCARD
3006
EXCEEDS RATE R?
3007
DELAY $\frac{W}{R}$ SECONDS
3008
GENERATE CKPT_N
3009
RX TABLE
3002
3000
W

FIG. 30

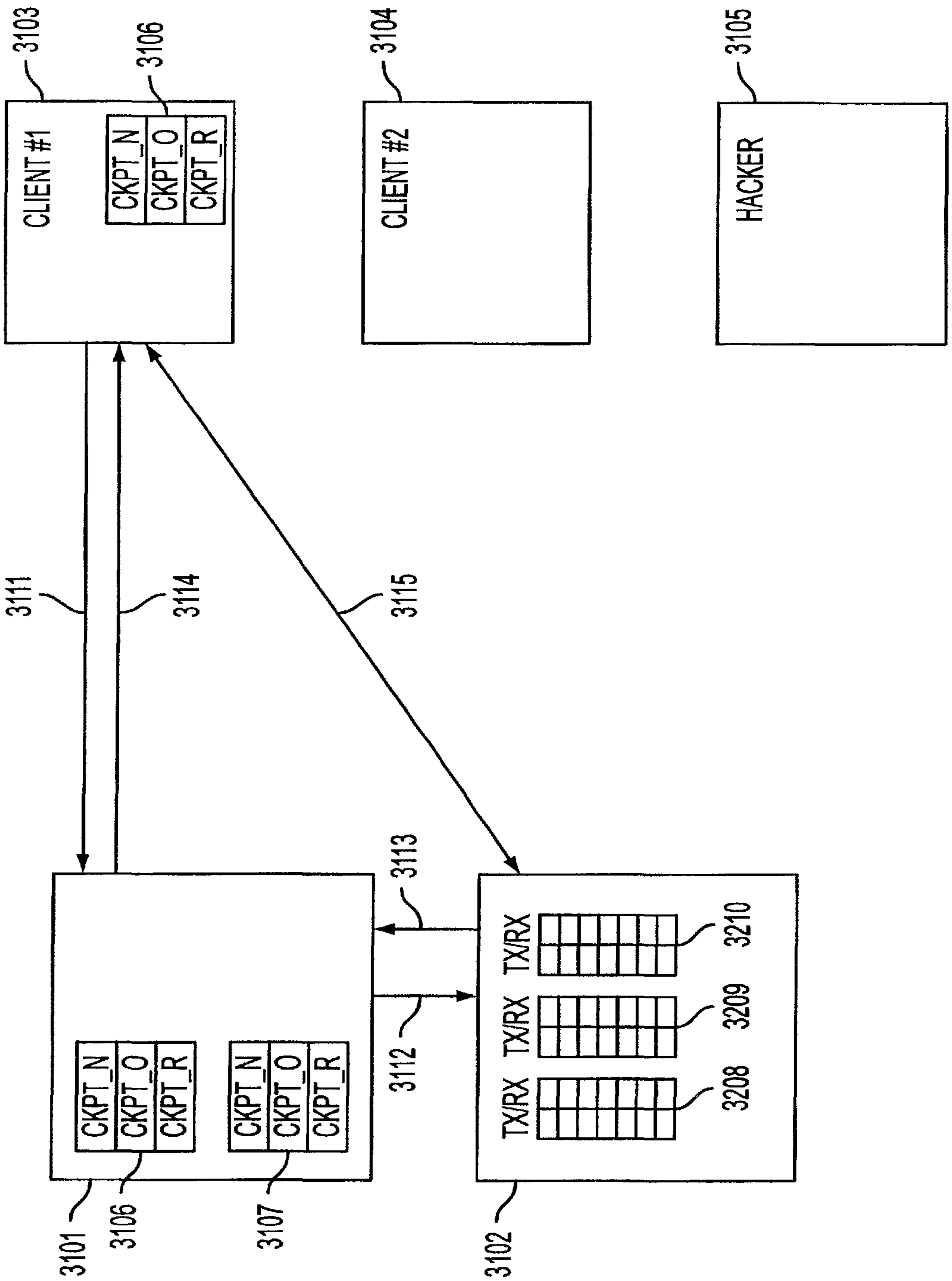

3103
CLIENT #1
3106
CKPT_N
CKPT_O
CKPT_R
3104
CLIENT #2
3105
HACKER
3111
3114
3115
3113
3112
TX/RX
TX/RX
TX/RX
3208
3209
3210
CKPT_N
CKPT_O
CKPT_R
CKPT_N
CKPT_O
CKPT_R
3101
3106
3107
3102

FIG. 31

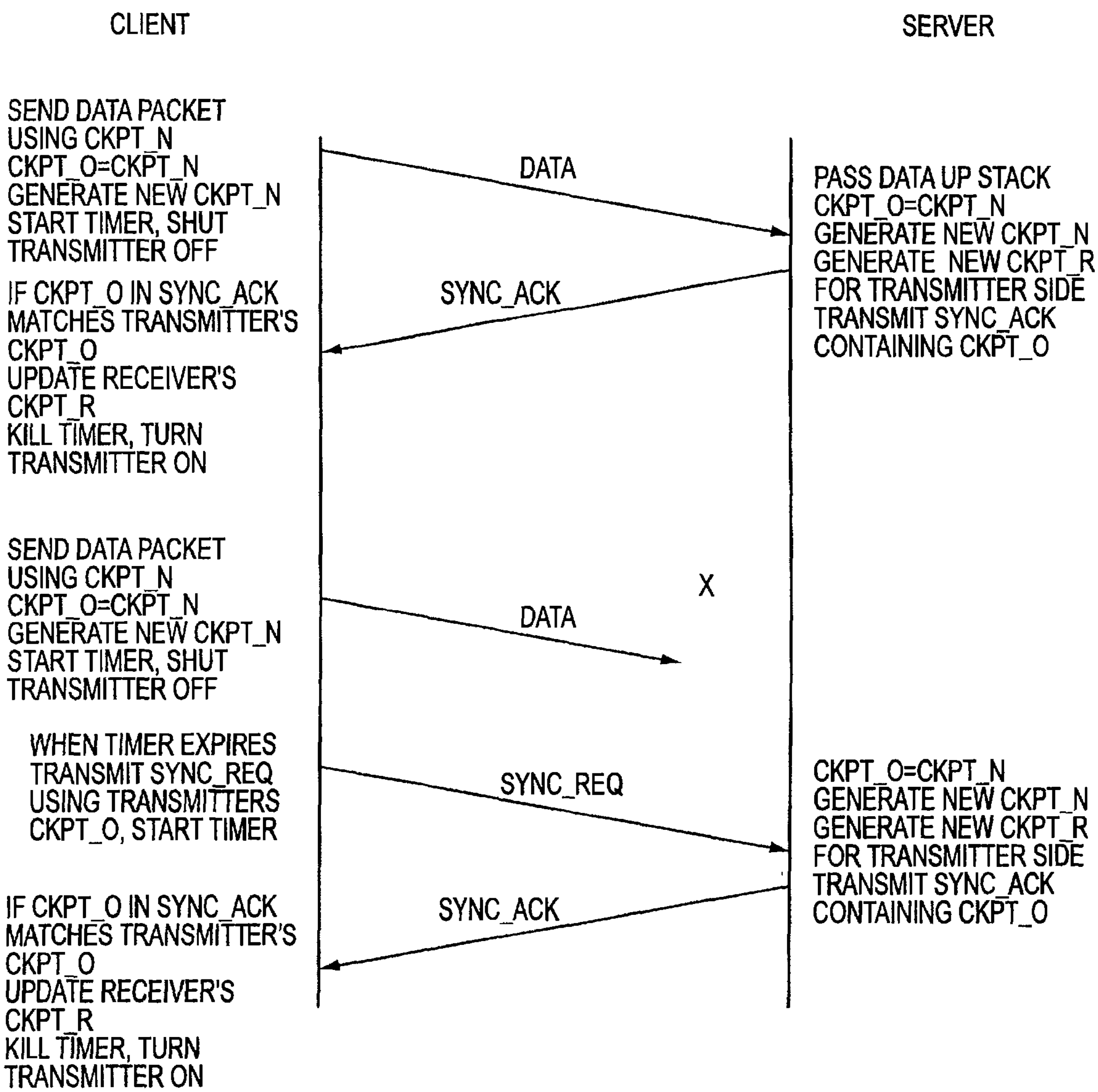

CLIENT
SERVER
SEND DATA PACKET
USING CKPT_N
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
START TIMER, SHUT
TRANSMITTER OFF
DATA
PASS DATA UP STACK
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
GENERATE NEW CKPT_R
FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING CKPT_O
SYNC_ACK
IF CKPT_O IN SYNC_ACK
MATCHES TRANSMITTER'S
CKPT_O
UPDATE RECEIVER'S
CKPT_R
KILL TIMER, TURN
TRANSMITTER ON
SEND DATA PACKET
USING CKPT_N
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
START TIMER, SHUT
TRANSMITTER OFF
X
DATA
WHEN TIMER EXPIRES
TRANSMIT SYNC_REQ
USING TRANSMITTERS
CKPT_O, START TIMER
SYNC_REQ
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
GENERATE NEW CKPT_R
FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING CKPT_O
SYNC_ACK
IF CKPT_O IN SYNC_ACK
MATCHES TRANSMITTER'S
CKPT_O
UPDATE RECEIVER'S
CKPT_R
KILL TIMER, TURN
TRANSMITTER ON

FIG. 32

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority from and is a continuation-in-part of previously filed U.S. application Ser. No. 09/429,643, filed on Oct. 29, 1999. The subject matter of that application, which is bodily incorporated herein, derives from provisional U.S. application No. 60/106,261 (filed Oct. 30, 1998) and No. 60/137,704 (filed Jun. 7, 1999).

BACKGROUND OF THE INVENTION

A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. **1**. Two terminals, an originating terminal **100** and a destination terminal **110** are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal **100** may transmit secret information to terminal **110** over the Internet **107**. Also, it may be desired to prevent an eavesdropper from discovering that terminal **100** is in communication with terminal **110**. For example, if terminal **100** is a user and terminal **110** hosts a web site, terminal **100**'s user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web-sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

Data security is usually tackled using some form of data encryption. An encryption key **48** is known at both the originating and terminating terminals **100** and **110**. The keys may be private and public at the originating and destination terminals **100** and **110**, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

Still another anonymity technique, called 'crowds,' protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the "crowd" or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one layer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile

Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet **140** undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called agile routing. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

The IP address of a TARP router can be changed, a feature called IP agility. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Intercomection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IPT are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security.

Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to portion, or entirety, of a message, and that portion or entirety then interleaved into a number of separate packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an illustration of secure communications over the Internet according to a prior art embodiment.

FIG. **2** is an illustration of secure communications over the Internet according to a an embodiment of the invention.

FIG. **3***a* is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

FIG. **3***b* is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

FIG. **4** is an illustration of an OSI layer location of processes that may be used to implement the invention.

FIG. **5** is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

FIG. **6** is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

FIG. **7** is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

FIG. **8** shows how a secure session is established and synchronized between a client and a TARP router.

FIG. **9** shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

FIG. **10** shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

FIG. **11** shows how multiple IP packets can be embedded into a single "frame" such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

FIG. **12**A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

FIG. **12**B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

FIG. **13** shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

FIG. **14** shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

FIG. **15** shows further details of the checkpoint scheme of FIG. **14**.

FIG. **16** shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

FIG. **17** shows a storage array for a receiver's active addresses.

FIG. **18** shows the receiver's storage array after receiving a sync request.

FIG. 19 shows the receiver's storage array after new addresses have been generated.

FIG. 20 shows a system employing distributed transmission paths.

FIG. 21 shows a plurality of link transmission tables that can be used to route packets in the system of FIG. 20.

FIG. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

FIG. 22B shows a flowchart for setting a weight value to zero if a transmitter turns off.

FIG. 23 shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

FIG. 24 shows an example using the system of FIG. 23.

FIG. 25 shows a conventional domain-name look-up service.

FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation.

FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

FIG. 28 shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

FIG. 29 shows one embodiment of a system employing the principles of FIG. 28.

FIG. 30 shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

FIG. 31 shows a signaling server 3101 and a transport server 3102 used to establish a VPN with a client computer.

FIG. 32 shows message flows relating to synchronization protocols of FIG. 31.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. 2, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers 122–127 that are similar to regular IP routers 128–132 in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets 140. TARP packets 140 are identical to normal IP packet messages that are routed by regular IP routers 128–132 because each TARP packet 140 contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's 140 IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal 110. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet 140 since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal 110.

Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key 146. The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110. Each TARP router 122–127, using the link key 146 it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt using the link key 146 and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

Once the outer layer of decryption is completed by a TARP router 122–127, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet 140 to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet 140 to another TARP router 122–127 or to the destination TARP terminal 110. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to the destination TARP terminal 110. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to a TARP router 122–127 that the current TARP terminal chooses at random. As a result, each TARP packet 140 is routed through some minimum number of hops of TARP routers 122–127 which are chosen at random.

Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called agile routing. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IP_C. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers **122–127** intervening between the originating **100** and destination **110** TARP terminals. The session key is used to decrypt the payloads of the TARP packets **140** permitting an entire message to be reconstructed.

In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets **140** may be used as desired.

Referring to FIG. **3***a*, to construct a series of TARP packets, a data stream **300** of IP packets **207***a*, **207***b*, **207***c*, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments **1–9** are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets **207***a*–**207***c* used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the interleave window.

To create a packet, the transmitting software interleaves the normal IP packets **207***a* et. seq. to form a new set of interleaved payload data **320**. This payload data **320** is then encrypted using a session key to form a set of session-key-encrypted payload data **330**, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets **207***a*–**207***c*, new TARP headers IP_T are formed. The TARP headers IP_T can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IP_T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence.
2. An interleave sequence number—an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.
3. A time-to-live (TTL) datum—indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.
4. Data type identifier—indicates whether the payload contains, for example, TCP or UDP data.
5. Sender's address—indicates the sender's address in the TARP network.
6. Destination address—indicates the destination terminal's address in the TARP network.
7. Decoy/Real—an indicator of whether the packet contains real message data or dummy decoy data or a combination.

Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets **207***a*–**207***c* all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

Referring to FIG. **3***b*, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block **520** for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. **3***b*. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of FIG. **3***a*. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. **3***a*. The remaining process is as shown in, and discussed with reference to, FIG. **3***a*.

Once the TARP packets **340** are formed, each entire TARP packet **340**, including the TARP header IP_T, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header IP_C is added to each encrypted TARP packet **340** to form a normal IP packet **360** that can be transmitted to a TARP router. Note that the process of constructing the TARP packet **360** does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

Note that, TARP header IP_T could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. **4**, a TARP transceiver **405** can be an originating terminal **100**, a destination terminal

110, or a TARP router 122–127. In each TARP Transceiver 405, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver 405 is a router, the received TARP packets 140 are not processed into a stream of IP packets 415 because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal 110. The intervening process, a "TARP Layer" 420, could be combined with either the data link layer 430 or the Network layer 410. In either case, it would intervene between the data link layer 430 so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the Network layer 410. As an example of combining the TARP layer 420 with the data link layer 430, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrams as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

Decoy packets may be generated by each TARP terminal 100, 110 or each router 122–127 on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal 110 may generate decoy packets equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

Referring to FIG. 5, the following particular steps may be employed in the above-described method for routing TARP packets.

S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.

S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

S4. If the packet is a decoy packet, the perishable decoy counter is incremented.

S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.

S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.

S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.

S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.

S10. The TARP packet is encrypted using the memorized link key.

S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

Referring to FIG. **6**, the following particular steps may be employed in the above-described method for generating TARP packets.

S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.

S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.

S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.

S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.

S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.

S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

Referring to FIG. **7**, the following particular steps may be employed in the above-described method for receiving TARP packets.

S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.

S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

S44. If the packet is a decoy packet, the perishable decoy counter is incremented.

S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.

S46. The TARP packets are cached until all packets forming an interleave window are received.

S47. Once all packets of an interleave window are received, the packets are deinterleaved.

S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.

S49. The decrypted block is then divided using the window sequence data and the IP_T headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.

S50. The packets are then handed up to the IP layer processes.

1. SCALABILITY ENHANCEMENTS

The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

FIG. **8** shows how a client computer **801** and a TARP router **811** can establish a secure session. When client **801** seeks to establish an IHOP session with TARP router **811**, the client **801** sends "secure synchronization" request ("SSYN") packet **821** to the TARP router **811**. This SYN packet **821** contains the client's **801** authentication token, and may be sent to the router **811** in an encrypted format. The source and destination IP numbers on the packet **821** are the client's **801** current fixed IP address, and a "known" fixed IP address for the router **811**. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's **801** SSYN packet **821**, the router **811** responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") **822** to the client **801**. This SSYN ACK **822** will contain the transmit and receive hopblocks that the client **801** will use when communicating with the TARP router **811**. The client **801** will acknowledge the TARP router's **811** response packet **822** by generating an encrypted SSYN ACK ACK packet **823** which will be sent from the client's **801** fixed IP address and to the TARP router's **811** known fixed IP address. The client **801** will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet **824**, will be sent with the first {sender, receiver} IP pair in the client's transmit table **921** (FIG. **9**), as specified in the transmit hopblock provided by the TARP router **811** in the SSYN ACK packet **822**. The TARP router **811** will respond to the SSI packet **824** with an SSI ACK packet **825**, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table **923**. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client **801** and the TARP router **811** will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client **801** and TARP router **802** may re-establish the secure session by the procedure outlined in FIG. **8** and described above.

While the secure session is active, both the client **901** and TARP router **911** (FIG. **9**) will maintain their respective transmit tables **921**, **923** and receive tables **922**, **924**, as provided by the TARP router during session synchronization **822**. It is important that the sequence of IP pairs in the client's transmit table **921** be identical to those in the TARP router's receive table **924**; similarly, the sequence of IP pairs in the client's receive table **922** must be identical to those in the router's transmit table **923**. This is required for the session synchronization to be maintained. The client **901** need maintain only one transmit table **921** and one receive table **922** during the course of the secure session. Each sequential packet sent by the client **901** will employ the next {send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router **911** will expect each packet arriving from the client **901** to bear the next IP address pair shown in its receive table.

Since packets can arrive out of order, however, the router **911** can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router **911** to the client **901** are maintained in an identical manner; in particular, the router **911** will select the next IP address pair from its transmit table **923** when constructing a packet to send to the client **901**, and the client **901** will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link-based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based IP-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the {sender, receiver} IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of FIG. **9**; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in FIG. **10**, for example, client **1001** can establish three simultaneous sessions with each of three TARP routers provided by different ISPs **1011**, **1012**, **1013**. As an example, the client **1001** can use three different telephone lines **1021**, **1022**, **1023** to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of-service attacks and traffic monitoring.

2. FURTHER EXTENSIONS

The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self-synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. **11**, for example, a first Ethernet frame **1150** comprises a frame header **1101** and two embedded IP packets IP1 and IP2, while a second Ethernet frame **1160** comprises a different frame header **1104** and a single IP packet IP3. Each frame header generally includes a source hardware address **1101A** and a destination hardware address **1101B**; other well-known fields in frame headers are omitted from FIG. **11** for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

FIG. **12**A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

As shown in FIG. **12**A, two computer nodes **1201** and **1202** communicate over a communication channel such as an Ethernet. Each node executes one or more application programs **1203** and **1218** that communicate by transmitting packets through communication software **1204** and **1217**, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software **1204** and **1217** can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

The lowest levels of communication software **1204** and **1217** communicate with hardware components **1206** and **1214** respectively, each of which can include one or more registers **1207** and **1215** that allow the hardware to be reconfigured or controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process every incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack—otherwise it is discarded.

One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical-layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course-e.g., if all of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

Reference will now be made to FIGS. **12**A and **12**B in order to describe the many combinations and features that follow the inventive principles. As explained above, two computer nodes **1201** and **1202** are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (**1204** and **1217**, respectively) contains a modified element **1205** and **1216** that performs certain functions that deviate from the standard communication protocols. In particular, computer node **1201** implements a first "hop" algorithm **1208**X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node **1201** maintains a transmit table **1208** containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node **1202**. As each new IP packet is formed, the next sequential entry out of the sender's transmit table **1208** is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

At the receiving node **1202**, the same IP hop algorithm **1222X** is maintained and used to generate a receive table **1222** that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table **1208** matching the second five entries of receive table **1222**. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node **1202** maintains a receive window **W3** that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window **W3** slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window **W3** will be accepted; those falling outside of window **W3** will be rejected as invalid. The length of window **W3** can be adjusted as necessary to reflect network delays or other factors.

Node **1202** maintains a similar transmit table **1221** for creating IP packets and frames destined for node **1201** using a potentially different hopping algorithm **1221X**, and node **1201** maintains a matching receive table **1209** using the same algorithm **1209X**. As node **1202** transmits packets to node **1201** using seemingly random IP source, IP destination, and/or discriminator fields, node **1201** matches the incoming packet values to those falling within window WI maintained in its receive table. In effect, transmit table **1208** of node **1201** is synchronized (i.e., entries are selected in the same order) to receive table **1222** of receiving node **1202**. Similarly, transmit table **1221** of node **1202** is synchronized to receive table **1209** of node **1201**. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. 12A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node **1201** further maintains a transmit table **1210** using a transmit algorithm **1210X** to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields **1101**A and **1101**B in FIG. **11**) that are synchronized to a corresponding receive table **1224** at node **1202**. Similarly, node **1202** maintains a different transmit table **1223** containing source and destination hardware addresses that is synchronized with a corresponding receive table **1211** at node **1201**. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

FIG. **12**B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node.

Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks. (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. 12A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space

Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "dead-man" timer that expires after a certain period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N−1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair—and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

The aforementioned scheme may have some inherent security issues associated with it—namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair; this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This implementation is shown in FIG. **13**, where (for example) a first ISP **1302** is the sender and a second ISP **1303** is the receiver. (Other alternatives are possible from FIG. **13**.) A transmitted packet comprises a public or "outer" header **1305** that is not encrypted, and a private or "inner" header **1306** that is encrypted using for example a link key. Outer header **1305** includes a public sync portion while inner header **1306** contains the private sync portion. A receiving node decrypts the inner header using a decryption function **1307** in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step **1308**.) The public and decrypted private sync portions are combined in function **1308** in order to generate the combined sync **1309**. The combined sync (**1309**) is then fed into the RNG (**1310**) and compared to the IP address pair (**1311**) to validate or reject the packet.

An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent—even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large-integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. 14):

1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.
2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.
3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14).

When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. 15. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send sync_reqs until it receives a sync_ack, at which point transmission is reestablished.

From the receiver's perspective, the scheme operates as follows: (1) when it receives a "sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will be ignored if the synchronization has been established or it it will actually help to re-establish synchronization.

A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to be advanced by many steps during resynchronization. In this case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead Capability

An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead n steps efficiently. An LCR generates random numbers $X_1, X_2, X_3 \ldots X_k$ starting with seed X_0 using a recurrence

$$X_i=(aX_{i-1}+b)\bmod c, \tag{1}$$

where a, b and c define a particular LCR. Another expression for X_i,

$$X_i=((a^i(X_0+b)-b)/(a-1))\bmod c \tag{2}$$

enables the jump-ahead capability. The factor a^i can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as:

$$X_i=(a^i(X_0(a-1)+b)-b)/(a-1)\bmod c. \tag{3}$$

It can be shown that:

$$(a^i(X_0(a-1)+b)-b)/(a-1)\bmod c=((a^i \bmod((a-1)c)(X_0(a-1)+b)-b)/(a-1))\bmod c \tag{4}$$

$(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as b mod c and compute $a^i \bmod((a-1)c)$ (this requires O(log(i)) steps).

A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every n packets. The window would commence n IP pairs from the start of the previous window. Using X_j^w, the random number at the j^{th} checkpoint, as X_0 and n as i, a node can store $a^n \bmod((a-1)c)$ once per LCR and set

$$X_{j+1}^w=X_{n(j+1)}=((a^n \bmod((a-1)c)(X_j^w(a-1)+b)-b)/(a-1))\bmod c, \tag{5}$$

to generate the random number for the $j+1^{th}$ synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n).

Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme. An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack—against the encryptor.

F. Random Number Generator Example

Consider a RNG where a=31, b=4 and c=15. For this case equation (1) becomes:

$$X_i=(31X_{i-1}+4)\text{mod } 15. \quad (6)$$

If one sets $X_0=1$, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence $a^n=31^3=29791$, $c*(a-1)=15*30=450$ and $a^n \text{ mod}((a-1)c)=31^3 \text{ mod}(15*30)=29791 \text{ mod}(450)=91$. Equation (5) becomes:

$$((91(X_i30+4)-4)/30)\text{mod } 15 \quad (7).$$

Table 1 shows the jump ahead calculations from (7) . The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	$(X_i30 + 4)$	91 $(X_i30 + 4) - 4$	((91 $(X_i30 + 4) - 4)/30$	X_{i+3}
1	5	154	14010	467	2
4	2	64	5820	194	14
7	14	424	38580	1286	11
10	11	334	30390	1013	8
13	8	244	22200	740	5

G. Fast Packet Filter

Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet filtering is an important feature for implementing VPNs on shared media such as Ethernet.

Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.
2. There are 2^{24} (~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).
3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B-trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n-1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the x^{th} bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a 1, which will be referred to as the "test."

For example, suppose one wanted to represent the number **135** using a presence vector. The 135^{th} bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135^{th} bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector (s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. **16**). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

A presence vector will have a 1 in the y^{th} bit if and only if one or more addresses with a corresponding field of y are active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

I. Further Synchronization Enhancements

A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2×WINDOW_SIZE+OoO active addresses ($1 \leqq OoO \leqq WINDOW\_SIZE$ and $WINDOW\_SIZE \geqq 1$). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. 17 depicts a storage array for a receiver's active addresses.

The receiver starts with the first 2×WINDOW_SIZE addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as "used" and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last initial transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver's array might look like FIG. 18 when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

FIG. 19 shows the receiver's array after the new addresses have been generated. If the transmitter does not receive a SYNC_ACK, it will re-issue the SYNC_REQ at regular intervals. When the transmitter receives a SYNC_ACK, the packet counter is decremented by WINDOW_SIZE. If the packet counter reaches 2×WINDOW_SIZE—OoO then the transmitter ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

1. There is no need for an efficient jump ahead in the random number generator,
2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
3. No timer based re-synchronization is necessary. This is a consequence of 2.
4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

Another embodiment incorporating various inventive principles is shown in FIG. 20. In this embodiment, a message transmission system includes a first computer 2001 in communication with a second computer 2002 through a network 2011 of intermediary computers. In one variant of this embodiment, the network includes two edge routers 2003 and 2004 each of which is linked to a plurality of Internet Service Providers (ISPs) 2005 through 2010. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. 20, which is a representative configuration only and is not intended to be limiting. Each connection between ISPs is labeled in FIG. 20 to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element 2005) to ISP D (element 2008)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

As shown in FIG. 21, computer 2001 or edge router 2003 incorporates a plurality of link transmission tables 2100 that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet. For example, AD table 2101 contains a plurality of IP source/destination pairs that are randomly or quasi-randomly generated. When a packet is to be transmitted from first computer 2001 to second computer 2002, one of the link tables is randomly (or quasi-randomly) selected, and the next valid source/destination address pair from that table is used to transmit the packet through the network. If path AD is randomly selected, for example, the next source/destination IP address pair (which is pre-determined to transmit between ISP A (element 2005) and ISP B (element 2008)) is used to transmit the packet. If one of the transmission paths becomes degraded or inoperative, that link table can be set to a "down" condition as shown in table 2105, thus preventing addresses from being selected from that table. Other transmission paths would be unaffected by this broken link.

3. CONTINUATION-IN-PART IMPROVEMENTS

The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities. Each is discussed separately below.

A. Load Balancer

Various embodiments described above include a system in which a transmitting node and a receiving node are coupled through a plurality of transmission paths, and wherein successive packets are distributed quasi-randomly over the plurality of paths. See, for example, FIGS. 20 and 21 and accompanying description. The improvement extends this basic concept to encompass distributing packets across different paths in such a manner that the loads on the paths are generally balanced according to transmission link quality.

In one embodiment, a system includes a transmitting node and a receiving node that are linked via a plurality of transmission paths having potentially varying transmission quality. Successive packets are transmitted over the paths based on a weight value distribution function for each path. The rate that packets will be transmitted over a given path can be different for each path. The relative "health" of each transmission path is monitored in order to identify paths that have become degraded. In one embodiment, the health of each path is monitored in the transmitter by comparing the number of packets transmitted to the number of packet acknowledgements received. Each transmission path may comprise a physically separate path (e.g., via dial-up phone line, computer network, router, bridge, or the like), or may comprise logically separate paths contained within a broadband communication medium (e.g., separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link).

When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the synchronization function (i.e., no packets are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

Conventional TCP/IP protocols include a "throttling" feature that reduces the transmission rate of packets when it is determined that delays or errors are occurring in transmission. In this respect, timers are sometimes used to determine whether packets have been received. These conventional techniques for limiting transmission of packets, however, do not involve multiple transmission paths between two nodes wherein transmission across a particular path relative to the others is changed based on link quality.

According to certain embodiments, in order to damp oscillations that might otherwise occur if weight distributions are changed drastically (e.g., according to a step function), a linear or an exponential decay formula can be applied to gradually decrease the weight value over time that a degrading path will be used. Similarly, if the health of a degraded path improves, the weight value for that path is gradually increased.

Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over time for a path, one specific implementation uses the "windowing" concepts described above to evaluate transmission path health.

The same scheme can be used to shift virtual circuit paths from an "unhealthy" path to a "healthy" one, and to select a path for a new virtual circuit.

FIG. **22**A shows a flowchart for adjusting weight values associated with a plurality of transmission links. It is assumed that software executing in one or more computer nodes executes the steps shown in FIG. **22**A. It is also assumed that the software can be stored on a computer-readable medium such as a magnetic or optical disk for execution by a computer.

Beginning in step **2201**, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

In step **2202**, a check is made to determine whether more than one transmitter (e.g., transmission path) is turned on. If not, the process is terminated and resumes at step **2201**.

In step **2203**, the link quality is compared to a given threshold (e.g., 50%, or any arbitrary number). If the quality falls below the threshold, then in step **2207** a check is made to determine whether the weight is above a minimum level (e.g., 1%). If not, then in step **2209** the weight is set to the minimum level and processing resumes at step **2201**. If the weight is above the minimum level, then in step **2208** the weight is gradually decreased for the path, then in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are increased).

If in step **2203** the quality of the path was greater than or equal to the threshold, then in step **2204** a check is made to determine whether the weight is less than a steady-state value for that path. If so, then in step **2205** the weight is increased toward the steady-state value, and in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are decreased). If in step **2204** the weight is not less than the steady-state value, then processing resumes at step **2201** without adjusting the weights.

The weights can be adjusted incrementally according to various functions, preferably by changing the value gradually. In one embodiment, a linearly decreasing function is used to adjust the weights; according to another embodiment, an exponential decay function is used. Gradually changing the weights helps to damp oscillators that might otherwise occur if the probabilities were abruptly.

Although not explicitly shown in FIG. **22**A the process can be performed only periodically (e.g., according to a time schedule), or it can be continuously run, such as in a background mode of operation. In one embodiment, the combined weights of all potential paths should add up to unity (e.g., when the weighting for one path is decreased, the corresponding weights that the other paths will be selected will increase).

Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

FIG. **22**B shows steps that can be executed to shut down transmission links where a transmitter turns off. In step **2210**, a transmitter shut-down event occurs. In step **2211**, a test is made to determine whether at least one transmitter is still turned on. If not, then in step **2215** all packets are dropped until a transmitter turns on. If in step **2211** at least one transmitter is turned on, then in step **2212** the weight for the path is set to zero, and the weights for the remaining paths are adjusted accordingly.

FIG. **23** shows a computer node **2301** employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. **23** communicate over a plurality of separate physical transmission paths. As shown in FIG. **23**, four transmission paths **X1** through **X4** are defined for communicating between the two nodes. Each node includes a packet transmitter **2302** that operates in accordance with a transmit table **2308** as described above. (The packet transmitter could also operate without using the IP-hopping features described above, but the following description assumes that some form of hopping is employed in conjunction with the path selection mechanism.). The computer node also includes a packet receiver **2303** that operates in accordance with a receive table **2309**, including a moving window W that moves as valid packets are received. Invalid packets having source and destination addresses that do not fall within window W are rejected.

As each packet is readied for transmission, source and destination IP addresses (or other discriminator values) are selected from transmit table **2308** according to any of the various algorithms described above, and packets containing these source/destination address pairs, which correspond to the node to which the four transmission paths are linked, are generated to a transmission path switch **2307**. Switch **2307**, which can comprise a software function, selects from one of the available transmission paths according to a weight distribution table **2306**. For example, if the weight for path **X1** is 0.2, then every fifth packet will be transmitted on path **X1**. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

Packet receiver **2303** generates an output to a link quality measurement function **2304** that operates as described above to determine the quality of each transmission path. (The input to packet receiver **2303** for receiving incoming packets is omitted for clarity). Link quality measurement function **2304** compares the link quality to a threshold for each transmission link and, if necessary, generates an output to weight adjustment function **2305**. If a weight adjustment is required, then the weights in table **2306** are adjusted accordingly, preferably according to a gradual (e.g., linearly or exponentially declining) function. In one embodiment, the weight values for all available paths are initially set to the same value, and only when paths degrade in quality are the weights changed to reflect differences.

Link quality measurement function **2304** can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function **2304**. According to one embodiment, load balancing is performed using information garnered during the normal synchronization, augmented slightly to communicate link health from the receiver to the transmitter. The receiver maintains a count, MESS_R(W), of the messages received in synchronization window W. When it receives a synchronization request (SYNC_REQ) corresponding to the end of window W, the receiver includes counter MESS_R in the resulting synchronization acknowledgement (SYNC_ACK) sent back to the transmitter. This allows the transmitter to compare messages sent to messages received in order to asses the health of the link.

If synchronization is completely lost, weight adjustment function **2305** decreases the weight value on the affected path to zero. When synchronization is regained, the weight value for the affected path is gradually increased to its original value. Alternatively, link quality can be measured by evaluating the length of time required for the receiver to acknowledge a synchronization request. In one embodiment, separate transmit and receive tables are used for each transmission path.

When the transmitter receives a SYNC_ACK, the MESS_R is compared with the number of messages transmitted in a window (MESS_T). When the transmitter receives a SYNC_ACK, the traffic probabilities will be examined and adjusted if necessary. MESS_R is compared with the number of messages transmitted in a window (MESS_T). There are two possibilities:

1. If MESS_R is less than a threshold value, THRESH, then the link will be deemed to be unhealthy. If the transmitter was turned off, the transmitter is turned on and the weight P for that link will be set to a minimum value MIN. This will keep a trickle of traffic on the link for monitoring purposes until it recovers. If the transmitter was turned on, the weight P for that link will be set to:

$$P' = \alpha \times \mathrm{MIN} + (1-\alpha) \times P \quad (1)$$

Equation 1 will exponentially damp the traffic weight value to MIN during sustained periods of degraded service.

2. If MESS_R for a link is greater than or equal to THRESH, the link will be deemed healthy. If the weight P for that link is greater than or equal to the steady state value S for that link, then P is left unaltered. If the weight P for that link is less than THRESH then P will be set to:

$$P' = \beta \times S + (1-\beta) \times P \quad (2)$$

where β is a parameter such that $0 <= \beta <= 1$ that determines the damping rate of P.

Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

A detailed example will now be provided with reference to FIG. **24**. As shown in FIG. **24**, a first computer **2401** communicates with a second computer **2402** through two routers **2403** and **2404**. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks).

Suppose that a first link **L1** can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link **L2** can sustain 75 Mb/s and has a window size of 24; and link **L3** can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200 Mb/s. The steady state traffic weights are 0.5 for link **L1**; 0.375 for link **L2**, and 0.125 for link **L3**. MIN=1 Mb/s, THRESH=0.8 MESS_T for each link, α=0.75 and β=0.5. These traffic weights will remain stable until a link stops for synchronization or reports a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link **L1** receives a SYNC_ACK containing a MESS_R of 24, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link **1** would be below THRESH (0.8). Consequently, link **L1**'s traffic weight value would be reduced to 0.12825, while link **L2**'s traffic weight value would be increased to 0.65812 and link **L3**'s traffic weight value would be increased to 0.217938.
2. Link **L2** and **L3** remained healthy and link **L1** stopped to synchronize. Then link **L1**'s traffic weight value would be set to 0, link **L2**'s traffic weight value would be set to 0.75, and link **L33**'s traffic weight value would be set to 0.25.
3. Link **L1** finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link **L1** would be below THRESH. Link **L1**'s traffic weight value would be increased to 0.005, link **L2**'s traffic weight value would be decreased to 0.74625, and link **L3**'s traffic weight value would be decreased to 0.24875.
4. Link **L1** received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T

(32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.2525, while link L2's traffic weight value would be decreased to 0.560625 and link L3's traffic weight value would be decreased to 0.186875.

5. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.37625; link L2's traffic weight value would be decreased to 0.4678125, and link L3's traffic weight value would be decreased to 0.1559375.

6. Link L1 remains healthy and the traffic probabilities approach their steady state traffic probabilities.

B. Use of a DNS Proxy to Transparently Create Virtual Private Networks

A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

This conventional scheme is shown in FIG. 25. A user's computer **2501** includes a client application **2504** (for example, a web browser) and an IP protocol stack **2505**. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack **2505**) to a DNS **2502** to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application **2504**, which is then able to use the IP address to communicate with the host **2503** through separate transactions such as PAGE REQ and PAGE RESP.

In the conventional architecture shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535).

The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

FIG. **26** shows a system employing various principles summarized above. A user's computer **2601** includes a conventional client (e.g., a web browser) **2605** and an IP protocol stack **2606** that preferably operates in accordance with an IP hopping function **2607** as outlined above. A modified DNS server **2602** includes a conventional DNS server function **2609** and a DNS proxy **2610**. A gatekeeper server **2603** is interposed between the modified DNS server and a secure target site **2704**. An "unsecure" target site **2611** is also accessible via conventional IP protocols.

According to one embodiment, DNS proxy **2610** intercepts all DNS lookup functions from client **2605** and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy **2610** determines whether the user has sufficient security privileges to access the site. If so, DNS proxy **2610** transmits a message to gatekeeper **2603** requesting that a virtual private network be created between user computer **2601** and secure target site **2604**. In one embodiment, gatekeeper **2603** creates "hopblocks" to be used by computer **2601** and secure target site **2604** for secure communication. Then, gatekeeper **2603** communicates these to user computer **2601**. Thereafter, DNS proxy **2610** returns to user computer **2601** the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) **2604**, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Had the user requested lookup of a non-secure web site such as site **2611**, DNS proxy would merely pass through to conventional DNS server **2609** the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site **2611**. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy **2610** would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

Gatekeeper **2603** can be implemented on a separate computer (as shown in FIG. **26**) or as a function within modified DNS server **2602**. In general, it is anticipated that gatekeeper **2703** facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site **2604** are assumed to be equipped with a secure communication function such as an IP hopping function **2608**.

It will be appreciated that the functions of DNS proxy **2610** and DNS server **2609** can be combined into a single server for convenience. Moreover, although element **2602** is shown as combining the functions of two servers, the two servers can be made to operate independently.

FIG. **27** shows steps that can be executed by DNS proxy server **2610** to handle requests for DNS look-up for secure hosts. In step **2701**, a DNS look-up request is received for a target host. In step **2702**, a check is made to determine whether access to a secure host was requested. If not, then in step **2703** the DNS request is passed to conventional DNS server **2609**, which looks up the IP address of the target site and returns it to the user's application for further processing.

In step **2702**, if access to a secure host was requested, then in step **2704** a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper **2603** (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges.

If the user is not authorized to access the secure site, then a "host unknown" message is returned (step **2705**). If the user has sufficient security privileges, then in step **2706** a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

Some or all of the security functions can be embedded in gatekeeper **2603**, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy **2610** communicates with gatekeeper **2603** to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:

Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would reject the request, informing DNS proxy server **2610** that it was unable to find the target computer. The DNS proxy **2610** would then return a "host unknown" error message to the client.

Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server **2610**, which would check its rules and determine that no VPN is needed. Gatekeeper **2603** would then inform the DNS proxy server to forward the request to conventional DNS server **2609**, which would resolve the request and return the result to the DNS proxy server and then back to the client.

Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper **2603**. Gatekeeper **2603** would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server **2610** to return an error message to the client.

C. Large Link to Small Link Bandwidth Management

One feature of the basic architecture is the ability to prevent so-called "denial of service" attacks that can occur if a computer hacker floods a known Internet node with packets, thus preventing the node from communicating with other nodes. Because IP addresses or other fields are "hopped" and packets arriving with invalid addresses are quickly discarded, Internet nodes are protected against flooding targeted at a single IP address.

In a system in which a computer is coupled through a link having a limited bandwidth (e.g., an edge router) to a node that can support a much higher-bandwidth link (e.g., an Internet Service Provider), a potential weakness could be exploited by a determined hacker. Referring to FIG. **28**, suppose that a first host computer **2801** is communicating with a second host computer **2804** using the IP address hopping principles described above. The first host computer is coupled through an edge router **2802** to an Internet Service Provider (ISP) **2803** through a low bandwidth link (LOW BW), and is in turn coupled to second host computer **2804** through parts of the Internet through a high bandwidth link (HIGH BW). In this architecture, the ISP is able to support a high bandwidth to the internet, but a much lower bandwidth to the edge router **2802**.

Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer **2801** across high bandwidth link HIGH BW. Normally, host computer **2801** would be able to quickly reject the packets since they would not fall within the acceptance window permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer **2801**. Consequently, the link to host computer **2801** is effectively flooded before the packets can be discarded.

According to one inventive improvement, a "link guard" function **2805** is inserted into the high-bandwidth node (e.g., ISP **2803**) that quickly discards packets destined for a low-bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the high-bandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a valid non-VPN packet, it is passed with a lower quality of service (e.g., lower priority).

In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc 2401], the packets have IP protocols **420** and **421**. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, **2805**, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid.

According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP **2903** maintains a copy **2910** of the receive table used by host computer **2901**. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard **2805** validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc 2104].

According to another embodiment, separate VPNs (using, for example, hopblocks) can be established for communicating between the low-bandwidth node and the high-bandwidth node (i.e., packets arriving at the high-bandwidth node are converted into different packets before being transmitted to the low-bandwidth node).

As shown in FIG. **29**, for example, suppose that a first host computer **2900** is communicating with a second host computer **2902** over the Internet, and the path includes a high bandwidth link HIGH BW to an ISP **2901** and a low bandwidth link LOW BW through an edge router **2904**. In accordance with the basic architecture described above, first host computer **2900** and second host computer **2902** would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables **2905**, **2906**, **2912** and **2913**. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

Suppose that a nefarious computer hacker **2903** was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP **2901**, and that these packets are being forwarded over a low-bandwidth link. Hacker computer **2903** could thus "flood" packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer **3000** would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard **2911** would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of-service flood attack could, however, still disrupt non-VPN traffic.

According to one embodiment of the improvement, ISP **2901** maintains a separate VPN with first host computer **2900**, and thus translates packets arriving at the ISP into packets having a different IP header before they are transmitted to host computer **2900**. The cryptographic keys used to authenticate VPN packets at the link guard **2911** and the cryptographic keys used to encrypt and decrypt the VPN packets at host **2902** and host **2901** can be different, so that link guard **2911** does not have access to the private host data; it only has the capability to authenticate those packets.

According to yet a third embodiment, the low-bandwidth node can transmit a special message to the high-bandwidth node instructing it to shut down all transmissions on a particular IP address, such that only hopped packets will pass through to the low-bandwidth node. This embodiment would prevent a hacker from flooding packets using a single IP address. According to yet a fourth embodiment, the high-bandwidth node can be configured to discard packets transmitted to the low-bandwidth node if the transmission rate exceeds a certain predetermined threshold for any given IP address; this would allow hopped packets to go through. In this respect, link guard **2911** can be used to detect that the rate of packets on a given IP address are exceeding a threshold rate; further packets addressed to that same IP address would be dropped or transmitted at a lower priority (e.g., delayed).

D. Traffic Limiter

In a system in which multiple nodes are communicating using "hopping" technology, a treasonous insider could internally flood the system with packets. In order to prevent this possibility, one inventive improvement involves setting up "contracts" between nodes in the system, such that a receiver can impose a bandwidth limitation on each packet sender. One technique for doing this is to delay acceptance of a checkpoint synchronization request from a sender until a certain time period (e.g., one minute) has elapsed. Each receiver can effectively control the rate at which its hopping window moves by delaying "SYNC ACK" responses to "SYNC_REQ" messages.

A simple modification to the checkpoint synchronizer will serve to protect a receiver from accidental or deliberate overload from an internally treasonous client. This modification is based on the observation that a receiver will not update its tables until a SYNC_REQ is received on hopped address CKPT_N. It is a simple matter of deferring the generation of a new CKPT_N until an appropriate interval after previous checkpoints.

Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets. A compliant transmitter would not issue new SYNC_REQ messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate, each receiver could defer issuing a new CKPT_N until M×N×W/R seconds have elapsed since the last SYNC_REQ has been received and accepted. If the transmitter exceeds this rate between a pair of checkpoints, it will issue the new checkpoint before the receiver is ready to receive it, and the SYNC_REQ will be discarded by the receiver. After this, the transmitter will re-issue the SYNC_REQ every Ti seconds until it receives a SYNC_ACK. The receiver will eventually update CKPT_N and the SYNC_REQ will be acknowledged. If the transmission rate greatly exceeds the allowed rate, the transmitter will stop until it is compliant. If the transmitter exceeds the allowed rate by a little, it will eventually stop after several rounds of delayed synchronization until it is in compliance. Hacking the transmitter's code to not shut off only permits the transmitter to lose the acceptance window. In this case it can recover the window and proceed only after it is compliant again.

Two practical issues should be considered when implementing the above scheme:

1. The receiver rate should be slightly higher than the permitted rate in order to allow for statistical fluctuations in traffic arrival times and non-uniform load balancing.

2. Since a transmitter will rightfully continue to transmit for a period after a SYNC_REQ is transmitted, the algorithm above can artificially reduce the transmitter's bandwidth. If events prevent a compliant transmitter from synchronizing for a period (e.g. the network dropping a SYNC_REQ or a SYNC_ACK) a SYNC_REQ will be accepted later than expected. After this, the transmitter will transmit fewer than expected messages before encountering the next checkpoint. The new checkpoint will not have been activated and the transmitter will have to retransmit the SYNC_REQ. This will appear to the receiver as if the transmitter is not compliant. Therefore, the next checkpoint will be accepted late from the transmitter's perspective. This has the effect of reducing the transmitter's allowed packet rate until the transmitter transmits at a packet rate below the agreed upon rate for a period of time.

To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of M×N×W/R seconds after the last SYNC_REQ has been received and accepted, 2×M×N×W/R seconds after next to the last SYNC_REQ has been received and accepted, C×M×N×W/R seconds after $(C-1)^{th}$ to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

FIG. 30 shows a system employing the above-described principles. In FIG. 30, two computers **3000** and **3001** are assumed to be communicating over a network N in accordance with the "hopping" principles described above (e.g., hopped IP addresses, discriminator values, etc.). For the sake of simplicity, computer **3000** will be referred to as the receiving computer and computer **3001** will be referred to as the transmitting computer, although full duplex operation is of course contemplated. Moreover, although only a single transmitter is shown, multiple transmitters can transmit to receiver **3000**.

As described above, receiving computer **3000** maintains a receive table **3002** including a window W that defines valid IP address pairs that will be accepted when appearing in incoming data packets. Transmitting computer **3001** maintains a transmit table **3003** from which the next IP address pairs will be selected when transmitting a packet to receiving computer **3000**. (For the sake of illustration, window W is also illustrated with reference to transmit table **3003**). As transmitting computer moves through its table, it will eventually generate a SYNC_REQ message as illustrated in function **3010**. This is a request to receiver **3000** to synchronize the receive table **3002**, from which transmitter **3001** expects a response in the form of a CKPT_N (included as part of a SYNC_ACK message). If transmitting computer **3001** transmits more messages than its allotment, it will prematurely generate the SYNC_REQ message. (If it has been altered to remove the SYNC_REQ message generation altogether, it will fall out of synchronization since receiver **3000** will quickly reject packets that fall outside of window W, and the extra packets generated by transmitter **3001** will be discarded).

In accordance with the improvements described above, receiving computer **3000** performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. **30**. In step **3004**, receiving computer **3000** receives the SYNC_REQ message. In step **3005**, a check is made to determine whether the request is a duplicate. If so, it is discarded in step **3006**. In step **3007**, a check is made to determine whether the SYNC_REQ received from transmitter **3001** was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step **3008** the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

Otherwise, if the rate has not been exceeded, then in step **3109** the next CKPT_N value is calculated and inserted into the receiver's hopping table prior to the next SYNC_REQ from the transmitter **3101**. Transmitter **3101** then processes the SYNC_REQ in the normal manner.

E. Signaling Synchronizer

In a system in which a large number of users communicate with a central node using secure hopping technology, a large amount of memory must be set aside for hopping tables and their supporting data structures. For example, if one million subscribers to a web site occasionally communicate with the web site, the site must maintain one million hopping tables, thus using up valuable computer resources, even though only a small percentage of the users may actually be using the system at any one time. A desirable solution would be a system that permits a certain maximum number of simultaneous links to be maintained, but which would "recognize" millions of registered users at any one time. In other words, out of a population of a million registered users, a few thousand at a time could simultaneously communicate with a central server, without requiring that the server maintain one million hopping tables of appreciable size.

One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets. When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

FIG. **31** shows a system employing certain of the above-described principles. In FIG. **31**, a signaling server **3101** and a transport server **3102** communicate over a link. Signaling server **3101** contains a large number of small tables **3106** and **3107** that contain enough information to authenticate a communication request with one or more clients **3103** and **3104**. As described in more detail below, these small tables may advantageously be constructed as a special case of the synchronizing checkpoint tables described previously. Transport server **3102**, which is preferably a separate computer in communication with signaling server **3101**, contains a smaller number of larger hopping tables **3108**, **3109**, and **3110** that can be allocated to create a VPN with one of the client computers.

According to one embodiment, a client that has previously registered with the system (e.g., via a system administration function, a user registration procedure, or some other method) transmits a request for information from a computer (e.g., a web site). In one variation, the request is made using a "hopped" packet, such that signaling server **3101** will quickly reject invalid packets from unauthorized computers such as hacker computer **3105**. An "administrative" VPN can be established between all of the clients and the signaling server in order to ensure that a hacker cannot flood signaling server **3101** with bogus packets. Details of this scheme are provided below.

Signaling server **3101** receives the request **3111** and uses it to determine that client **3103** is a validly registered user. Next, signaling server **3101** issues a request to transport server **3102** to allocate a hopping table (or hopping algorithm or other regime) for the purpose of creating a VPN with client **3103**. The allocated hopping parameters are returned to signaling server **3101** (path **3113**), which then supplies the hopping parameters to client **3103** via path **3114**, preferably in encrypted form.

Thereafter, client **3103** communicates with transport server **3102** using the normal hopping techniques described above. It will be appreciated that although signaling server **3101** and transport server **3102** are illustrated as being two separate computers, they could of course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. **31** differently from as shown without departing from the inventive principles.

One advantage of the above-described architecture is that signaling server **3101** need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer **3105**. Larger data tables needed to perform the hopping and synchronization functions are instead maintained in a transport server **3102**, and a smaller number of these tables are needed since they are only allocated for "active" links. After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server **3102** or signaling server **3101**.

A more detailed description will now be provided regarding how a special case of the checkpoint synchronization feature can be used to implement the signaling scheme described above.

The signaling synchronizer may be required to support many (millions) of standing, low bandwidth connections. It therefore should minimize per-VPL memory usage while providing the security offered by hopping technology. In order to reduce memory usage in the signaling server, the data hopping tables can be completely eliminated and data can be carried as part of the SYNC_REQ message. The table used by the server side (receiver) and client side (transmitter) is shown schematically as element **3106** in FIG. **31**.

The meaning and behaviors of CKPT_N, CKPT_O and CKPT_R remain the same from the previous description, except that CKPT_N can receive a combined data and SYNC_REQ message or a SYNC_REQ message without the data.

The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer T1 noting CKPT_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.
2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and and other information (i.e user credentials) contained in the inner header. It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT R and transmits a SYNC ACK containing CKPT_O in its payload.
3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.
4. **T1** expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPT_O associated with the timer, it starts timer **T1** noting CKPT_O again, and a SYNC_REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.
5. When the server receives a SYNC_REQ on its CKPT_N it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.
6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

FIG. **32** shows message flows to highlight the protocol. Reading from top to bottom, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT N. This message is successfully received and a passed up the stack. It also synchronizes the receiver i.e, the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned on and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

Next, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is lost. The client side timer expires and as a result a SYNC_REQ is transmitted on the client side transmitter's CKPT_O (this will keep happening until the SYNC_ACK has been received at the client). The SYNC_REQ is successfully received at the server. It synchronizes the receiver i.e, the server loads CKPT_N into CKPT_O and generates a new

CKPT_N. it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

There are numerous other scenarios that follow this flow. For example, the SYNC_ACK could be lost. The transmitter would continue to re-send the SYNC_REQ until the receiver synchronizes and responds.

The above-described procedures allow a client to be authenticated at signaling server **3201** while maintaining the ability of signaling server **3201** to quickly reject invalid packets, such as might be generated by hacker computer **3205**. In various embodiments, the signaling synchronizer is really a derivative of the synchronizer. It provides the same protection as the hopping protocol, and it does so for a large number of low bandwidth connections.

What is claimed is:

1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

2. The method of claim 1, wherein steps (2) and (3) are performed at a DNS server separate from the client computer.

3. The method of claim 1, further comprising the step of:

(4) in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and returning the IP address to the client computer.

4. The method of claim 1, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request.

5. The method of claim 1, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request.

6. The method of claim 1, wherein step (3) comprises the step of establishing the VPN by creating an IP address hopping scheme between the client computer and the target computer.

7. The method of claim 1, wherein step (3) comprises the step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer.

8. The method of claim 1, wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site.

9. The method of claim 5, wherein step (3) comprises the step of transmitting a message to the client computer to determine whether the client computer is authorized to establish the VPN target computer.

10. A system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer, comprising:

a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested; and

a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server.

11. The system of claim 10, wherein the gatekeeper computer creates the VPN by establishing an IP address hopping regime that is used to pseudorandomly change IP addresses in packets transmitted between the client computer and the secure target computer.

12. The system of claim 10, wherein the gatekeeper computer determines whether the client computer has sufficient security privileges to create the VPN and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN.

13. A method of establishing communication between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers, the method comprising the steps of:

(1) in the central computer, receiving from one of the plurality of client computers a request to establish a connection;

(2) authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client;

(3) responsive to a determination that the request is from an authorized client, allocating resources to establish a virtual private link between the client and a second computer; and

(4) communicating between the authorized client and the second computer using the virtual private link.

14. The method of claim 13, wherein step (4) comprises the step of communicating according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence.

15. The method of claim 14, wherein step (4) comprises the step of comparing an Internet Protocol (IP) address in a header of each data packet to a table of valid IP addresses maintained in a table in the second computer.

16. The method of claim 15, wherein step (4) comprises the step of comparing the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window.

17. The method of claim 13, wherein step (2) comprises the step of using a checkpoint data structure that maintains synchronization of a periodically changing parameter known by the central computer and the client computer to authenticate the client.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,502,135 B1
DATED : December 31, 2002
INVENTOR(S) : Edmund Colby Munger et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page,
Item [56], **References Cited**, OTHER PUBLICATIONS, insert the following:

-- Search Report (dated 8/20/02), International Application No. PCT/US01/04340
Search Report (dated 8/23/02), International Application No. PCT/US01/13260
James E. Bellaire, "New Statement of Rules – Naming Internet Domains", Internet Newsgroup, July 30, 1995, 1 page.
D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, August 1, 1998, pages 22-25.
August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, Vol. 17, No. 4, 1998, pages 293-298.
Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, June 21, 1997, 4 pages. --

Column 48,
Line 2, "VPN target computer" has been replaced with -- VPN with the target computer --.

Signed and Sealed this

Ninth Day of September, 2003

JAMES E. ROGAN
Director of the United States Patent and Trademark Office

US006502135C1

(12) **INTER PARTES REEXAMINATION CERTIFICATE** (0271st)

United States Patent

Munger et al.

(10) **Number: US 6,502,135 C1**

(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

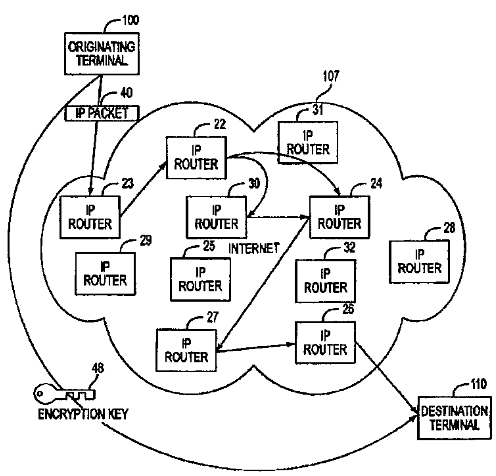
Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/draft302.txt on Feb. 4, 2002, 56 pages.

(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 Multi–path 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). (DNSSEC–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, "Buttet–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 Adminstrator'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).

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. Matehrs 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.

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:

(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.

* * * * *

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-270803**
(43)Date of publication of application : **14.10.1997**

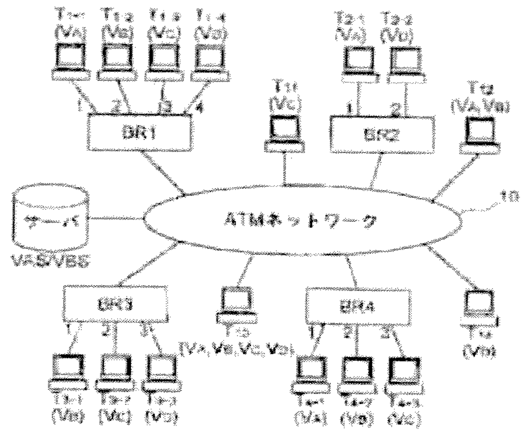
(51)Int.Cl.	**H04L 12/28**
	H04L 12/46
	H04L 12/66
	H04Q 3/00

(21)Application number :	**08-080005**	(71)Applicant :	**FURUKAWA ELECTRIC CO LTD:THE**
(22)Date of filing :	**02.04.1996**	(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.

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]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 BRI-BR4 is the same composition, it is represented here and shows an example of the ATM address table of bridge BRI 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

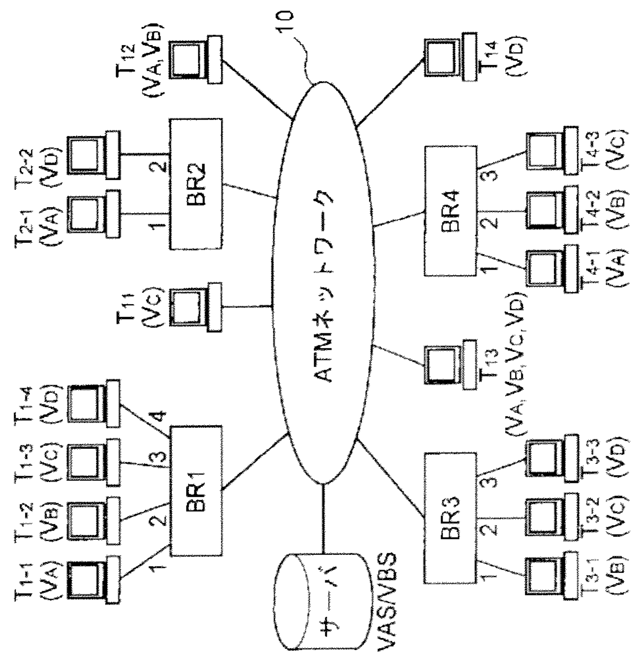
(72)発明者　堀口　政則
東京都千代田区丸の内２丁目６番１号　古河電気工業株式会社内

(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

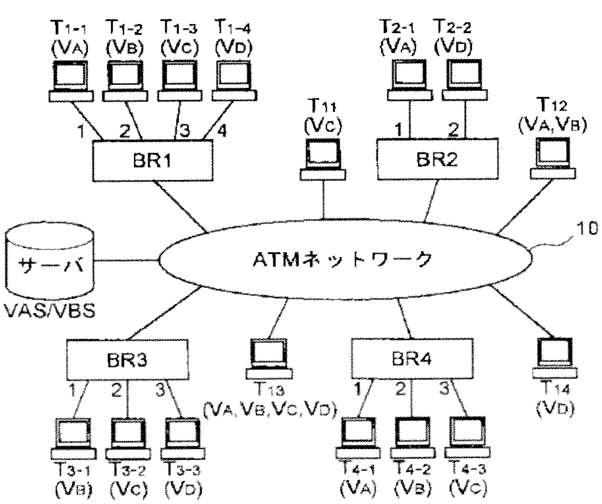
ＶＡＳ／ＡＢＳ　サーバ

ＢＲ1～ＢＲ4 ブリッジ

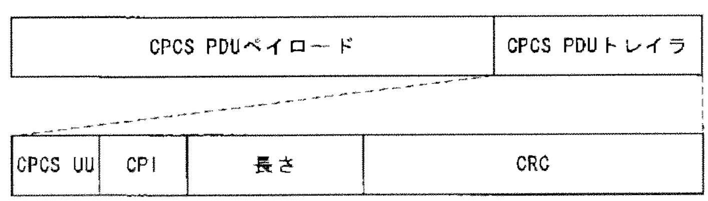
Ｔ11～Ｔ14　ＡＴＭ端末装置

Ｔ1-1～Ｔ1-4，Ｔ2-1，Ｔ2-2，Ｔ3-1～Ｔ3-3，Ｔ4-1～Ｔ4-3　ＬＡＮ端末装置

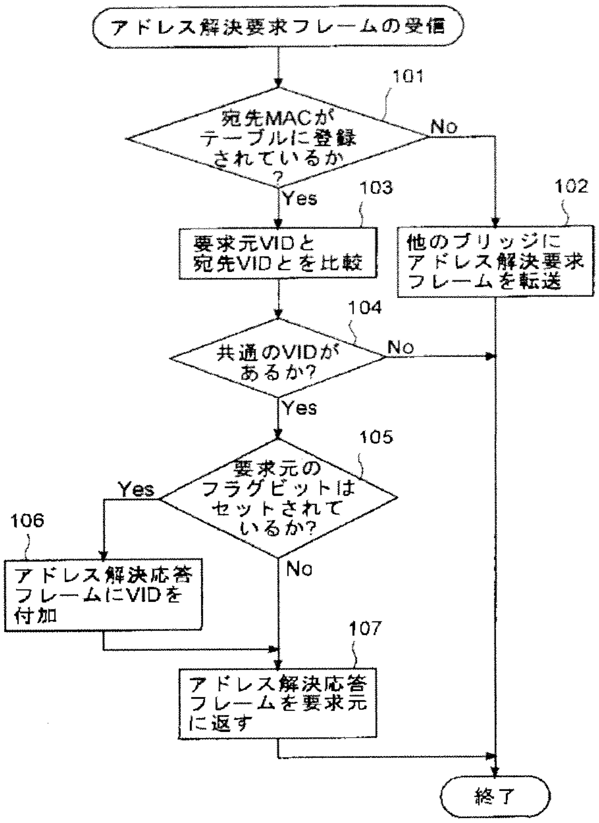
【図１】



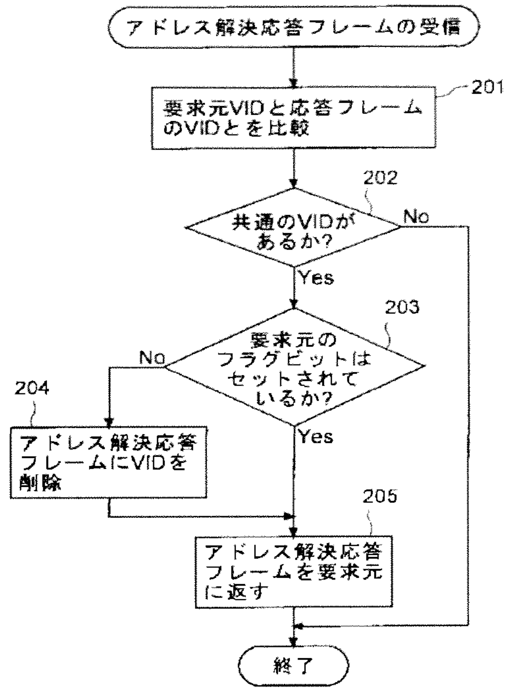
【図２】



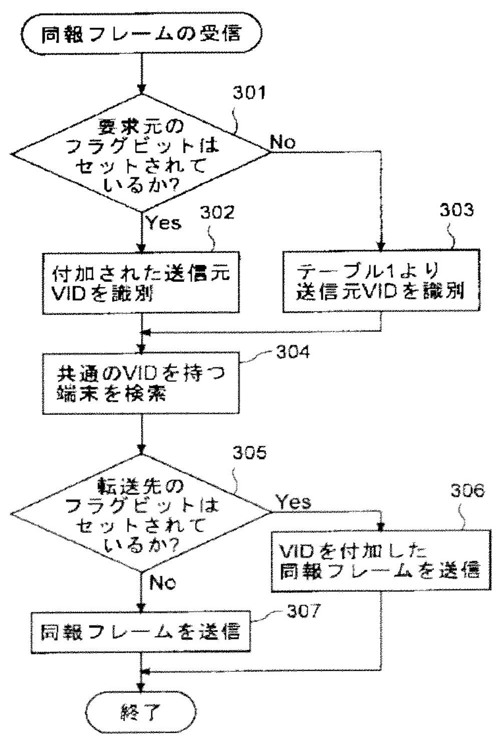
【図3】


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
アドレス解決応答フレームにVIDを付加
No
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
307
同報フレームを送信
終了

US006286047B1

(12) United States Patent
Ramanathan et al.

(10) Patent No.: US 6,286,047 B1
(45) Date of Patent: Sep. 4, 2001

(54) METHOD AND SYSTEM FOR AUTOMATIC DISCOVERY OF NETWORK SERVICES

(75) Inventors: Srinivas Ramanathan, Sunnyvale; Deborah L. Caswell, Santa Clara, both of CA (US)

(73) Assignee: Hewlett-Packard Company, Palo Alto, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/151,134

(22) Filed: Sep. 10, 1998

(51) Int. Cl.[7] G06F 15/16

(52) U.S. Cl. 709/224; 709/202; 709/217; 709/226; 345/329; 370/229; 370/254; 706/51; 707/501

(58) Field of Search 709/202, 203, 709/204, 205, 217, 218, 220, 224, 226, 227, 229; 345/329; 370/229, 230, 254, 258; 707/501; 706/51

(56) References Cited

U.S. PATENT DOCUMENTS

5,185,860		2/1993	Wu	395/200
5,276,789		1/1994	Besaw et al.	395/200
5,485,579	*	1/1996	Hitz et al. .	
5,644,720	*	7/1997	Boll et al. .	
5,678,045	*	10/1997	Bettels .	
5,727,147	*	3/1998	Van Hoff .	
5,740,362	*	4/1998	Buickel et al. .	
5,758,083	*	5/1998	Singh et al. .	
5,774,689	*	6/1998	Curtis et al. .	
5,781,534	*	7/1998	Perlman et al. .	
5,781,743	*	7/1998	Matsuno et al. .	
5,790,548	*	8/1998	Sistanizadeh et al. .	
5,793,965	*	8/1998	Vanderbilt et al.	709/203
5,796,951	*	8/1998	Hamner et al. .	
5,802,291	*	9/1998	Balick et al.	709/202
5,805,820	*	9/1998	Bellovin et al. .	

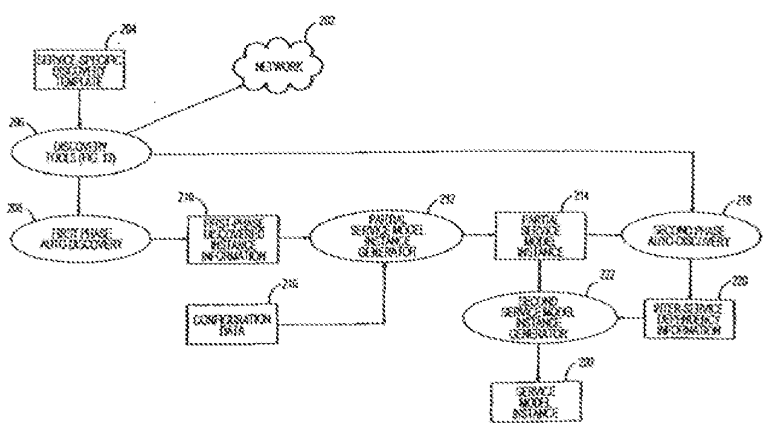
(List continued on next page.)

Primary Examiner—Robert B. Harrell
Assistant Examiner—Stephan Willett

(57) ABSTRACT

A method for identifying services, service elements and dependencies among the services and service elements includes executing first and second phases of discovery. In the first phase, the services and service elements are detected, as well as a first set of dependencies. The second phase is based on results of the first phase and is focused upon detecting inter-service dependencies, i.e., conditions in which proper operation of one service relies upon at least one other service. Various techniques may be used in executing the first phase, including accessing information in a domain name service (DNS) of the network to identify dependencies, as well as services and service elements. Discovery within the first phase may also be based upon recognizing naming conventions. Regarding the second phase, one approach to discovering inter-service dependencies is to deploy discovery agents implemented in computer software to access content of configuration files of applications detected in the first phase. Discovery agents may also be used to monitor connections completed via specified service elements detected in the first phase, such that other inter-service dependencies are identified. As an alternative or additional approach, network probes may be deployed to access information of data packets transmitted ted between service elements detected in the first phase, with the accessed packet information being used to detect inter-service dependencies. When information of the DNS is accessed in the first phase, the information is used as a basis for determining at least some of (1) groups of service elements that are generally equivalent with respect to executing a particular service within the network, (2) hosts supporting virtual hosting, (3) hosts supporting virtual servers, and (4) name servers.

20 Claims, 13 Drawing Sheets



VNET00221180

U.S. PATENT DOCUMENTS

5,812,771	* 9/1998	Fee et al. .	
5,835,718	* 11/1998	Blewett	709/218
5,854,901	* 12/1998	Cole et al. .	
5,862,339	* 1/1999	Bonnaure et al.	709/227
5,867,667	* 2/1999	Butman et al. .	
5,870,545	* 2/1999	Davis et al. .	
5,884,033	* 3/1999	Duvall et al. .	
5,913,041	* 6/1999	Ramanathan et al. .	
5,926,463	* 7/1999	Ahearn et al.	370/254
5,944,783	* 8/1999	Nieten	709/202
5,946,464	* 8/1999	Kito et al.	709/202
5,958,012	* 9/1999	Battat et al.	709/224
5,958,052	* 9/1999	Bellovin et al. .	
5,968,116	* 10/1999	Day, II et al.	709/202
5,978,594	* 11/1999	Bonnell et al. .	
5,983,233	* 11/1999	Potonniee .	
5,999,940	* 12/1999	Ranger .	
6,009,467	* 12/1999	Ratcliff et al.	709/220
6,012,066	* 1/2000	Discount et al. .	
6,014,686	* 1/2000	Elnozahy et al.	709/202
6,044,224	* 3/2000	Radia et al. .	
6,046,988	* 4/2000	Schenkel et al.	370/254
6,054,987	* 4/2000	Richardson .	
6,055,562	* 4/2000	Devarakonda et al.	709/202
6061721	* 5/2000	Ismael et al. .	
6,063,129	* 5/2000	Bentley et al. .	

* cited by examiner

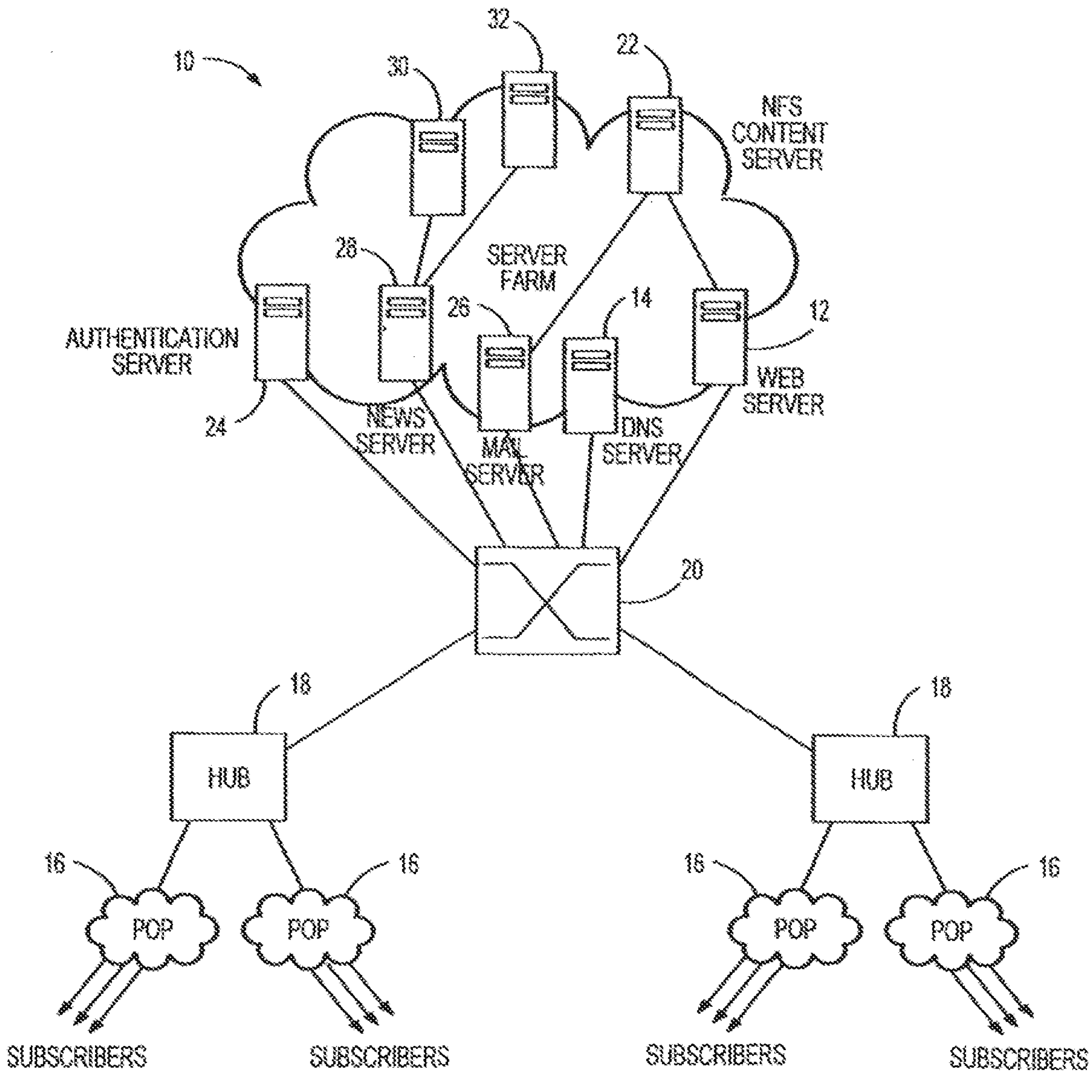


FIG. 1
(PRIOR ART)

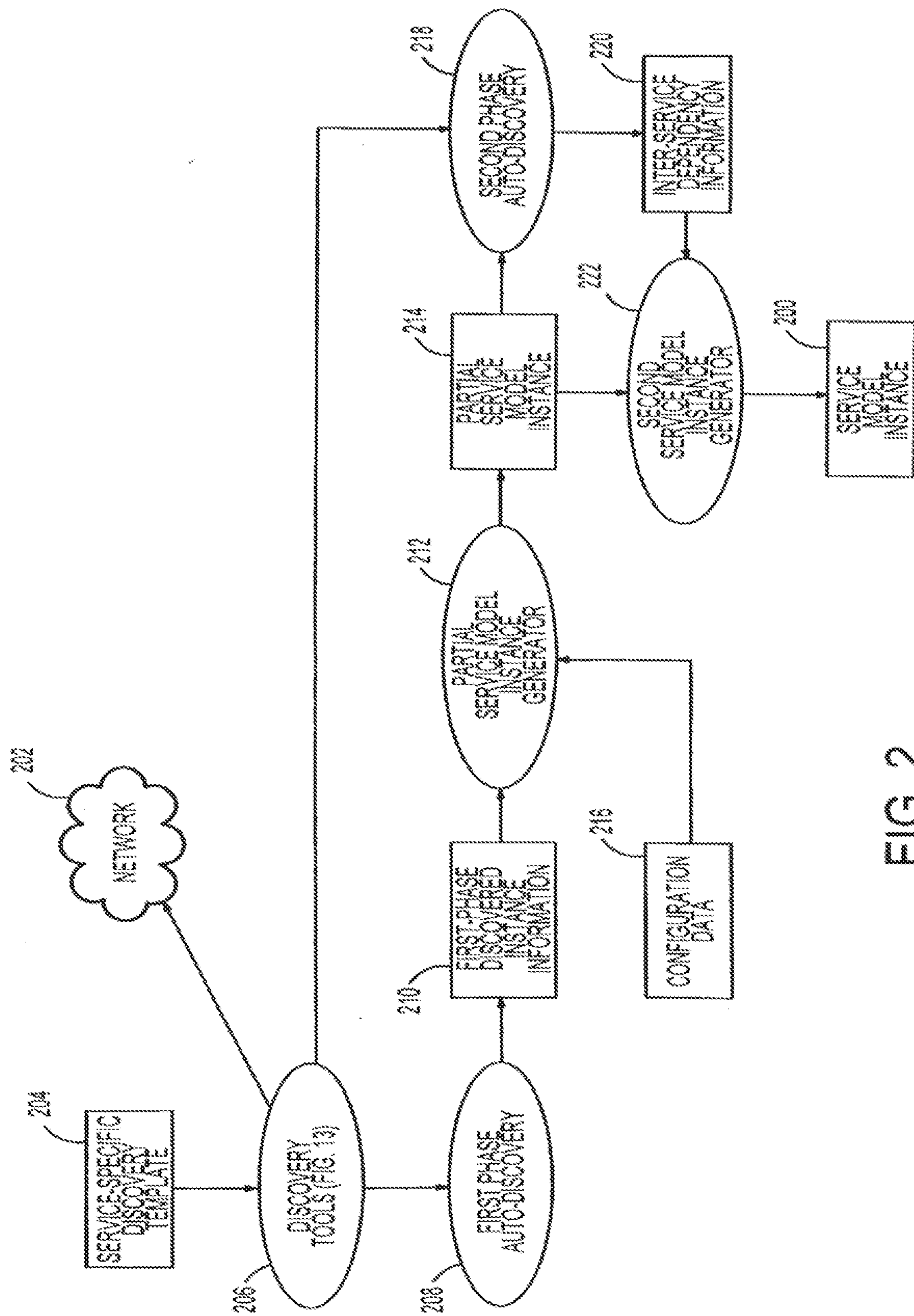
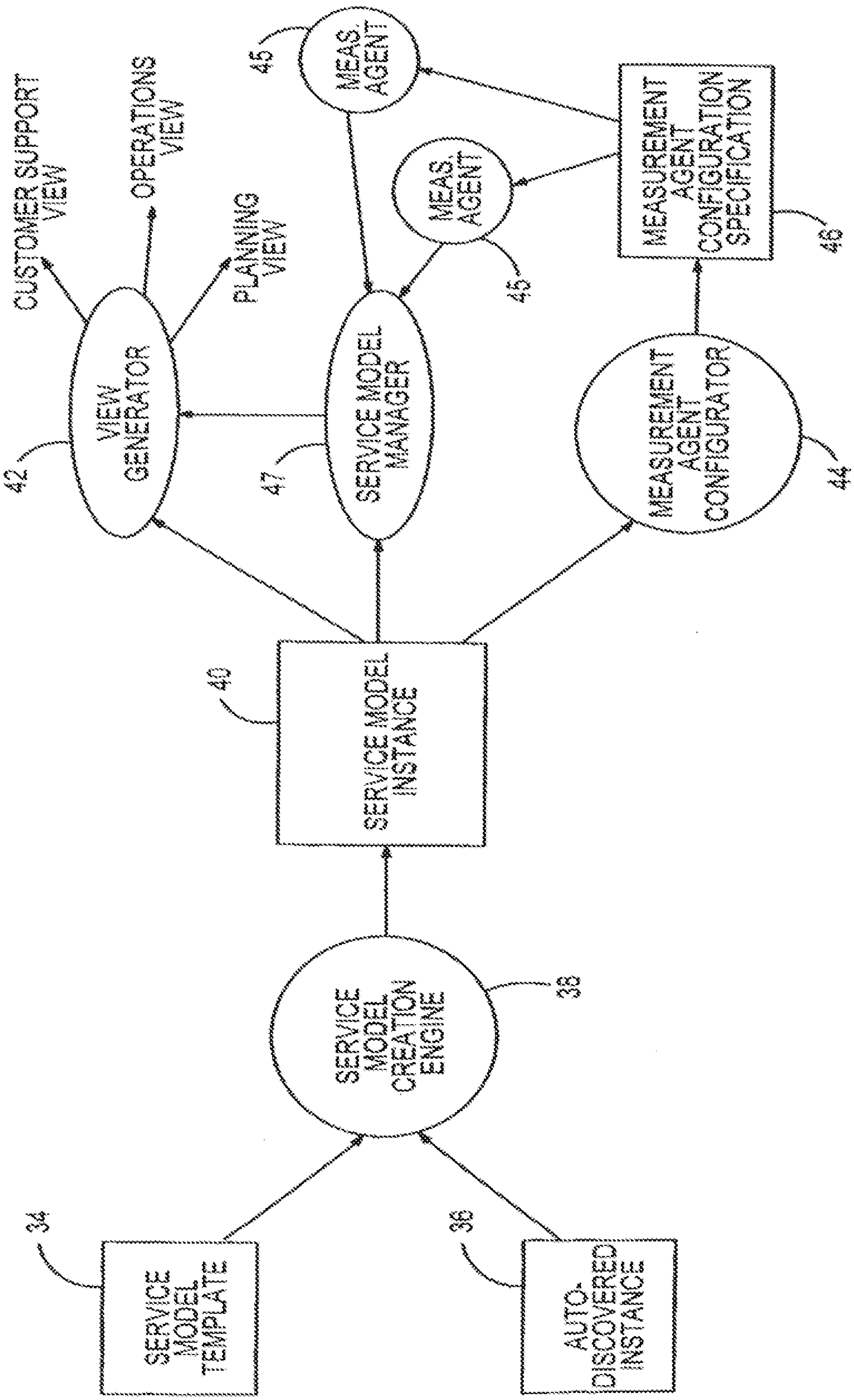

204
SERVICE-SPECIFIC DISCOVERY TEMPLATE
202
NETWORK
206
DISCOVERY TOOLS (FIG. 13)
208
FIRST PHASE AUTO-DISCOVERY
210
FIRST-PHASE DISCOVERED INSTANCE INFORMATION
216
CONFIGURATION DATA
212
PARTIAL SERVICE MODEL INSTANCE GENERATOR
214
PARTIAL SERVICE MODEL INSTANCE
218
SECOND PHASE AUTO-DISCOVERY
220
INTER-SERVICE DEPENDENCY INFORMATION
222
SECOND SERVICE MODEL INSTANCE GENERATOR
200
SERVICE MODEL INSTANCE

FIG. 2



SERVICE MODEL TEMPLATE
34
AUTO-DISCOVERED INSTANCE
36
SERVICE MODEL CREATION ENGINE
38
SERVICE MODEL INSTANCE
40
VIEW GENERATOR
42
CUSTOMER SUPPORT VIEW
OPERATIONS VIEW
PLANNING VIEW
SERVICE MODEL MANAGER
47
MEAS. AGENT
45
MEAS. AGENT
45
MEASUREMENT AGENT CONFIGURATOR
44
MEASUREMENT AGENT CONFIGURATION SPECIFICATION
46

FIG. 3

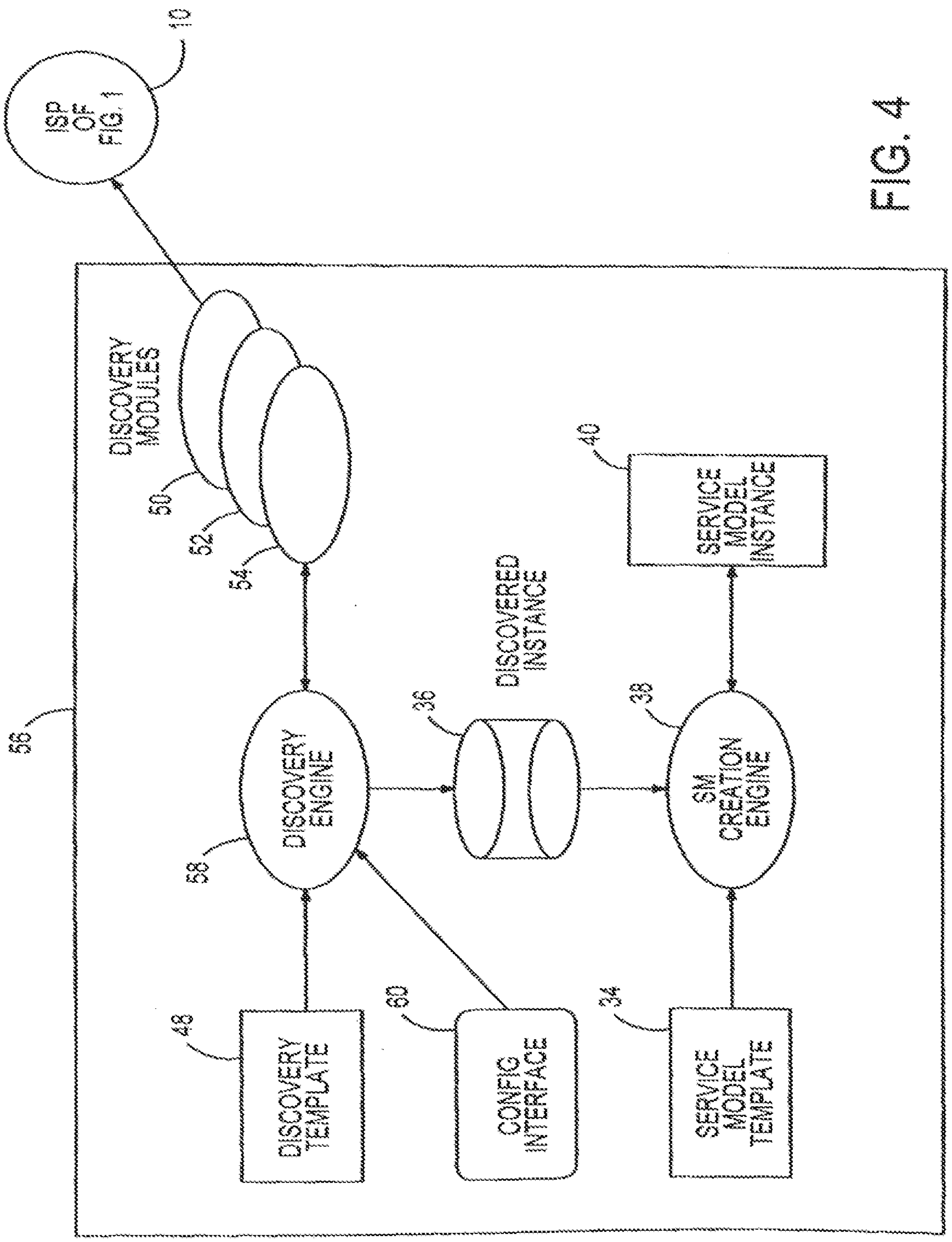

ISP OF FIG. 1
10
DISCOVERY MODULES
50
52
54
56
DISCOVERY ENGINE
58
DISCOVERED INSTANCE
36
SM CREATION ENGINE
38
SERVICE MODEL INSTANCE
40
DISCOVERY TEMPLATE
48
CONFIG INTERFACE
60
SERVICE MODEL TEMPLATE
34

FIG. 4

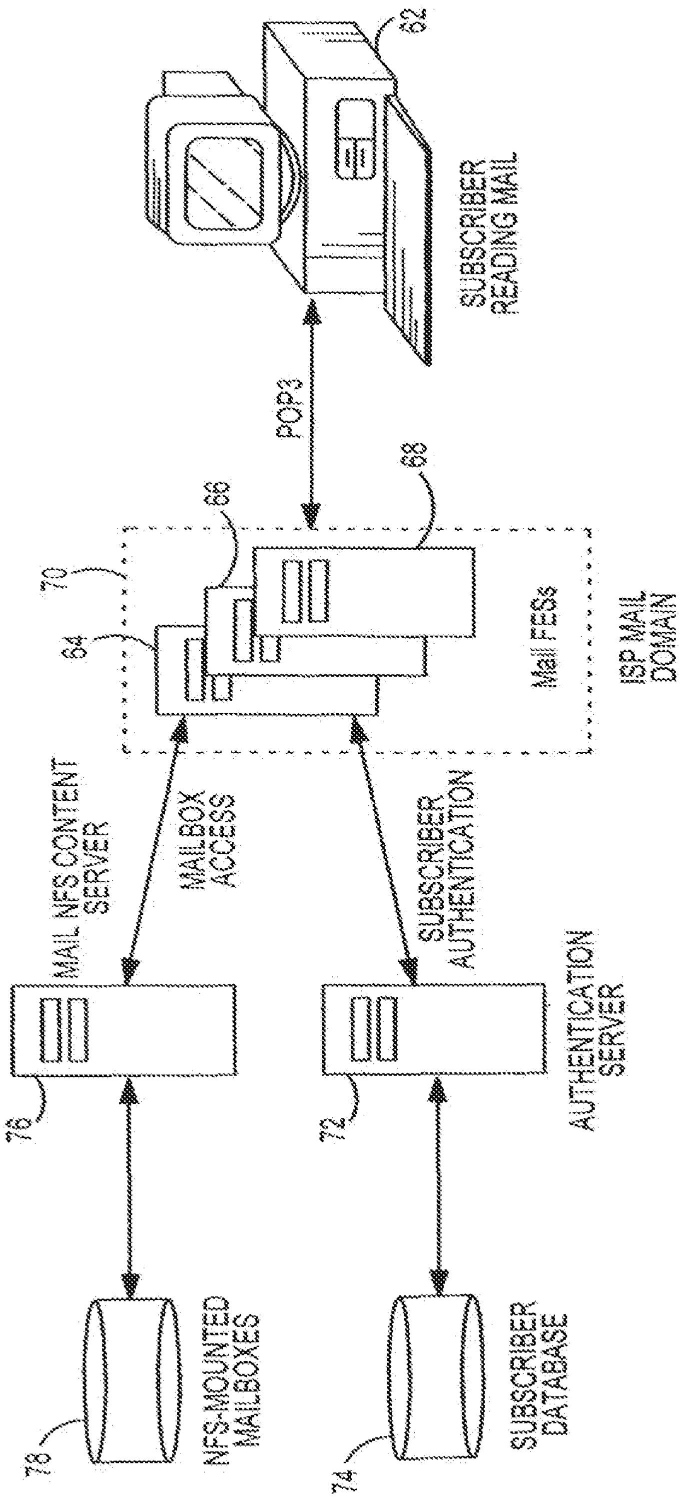

62
SUBSCRIBER
READING MAIL
POP3
70
64
66
68
Mail FESs
ISP MAIL
DOMAIN
MAIL NFS CONTENT
SERVER
MAILBOX
ACCESS
SUBSCRIBER
AUTHENTICATION
76
72
AUTHENTICATION
SERVER
78
NFS-MOUNTED
MAILBOXES
74
SUBSCRIBER
DATABASE

FIG. 5

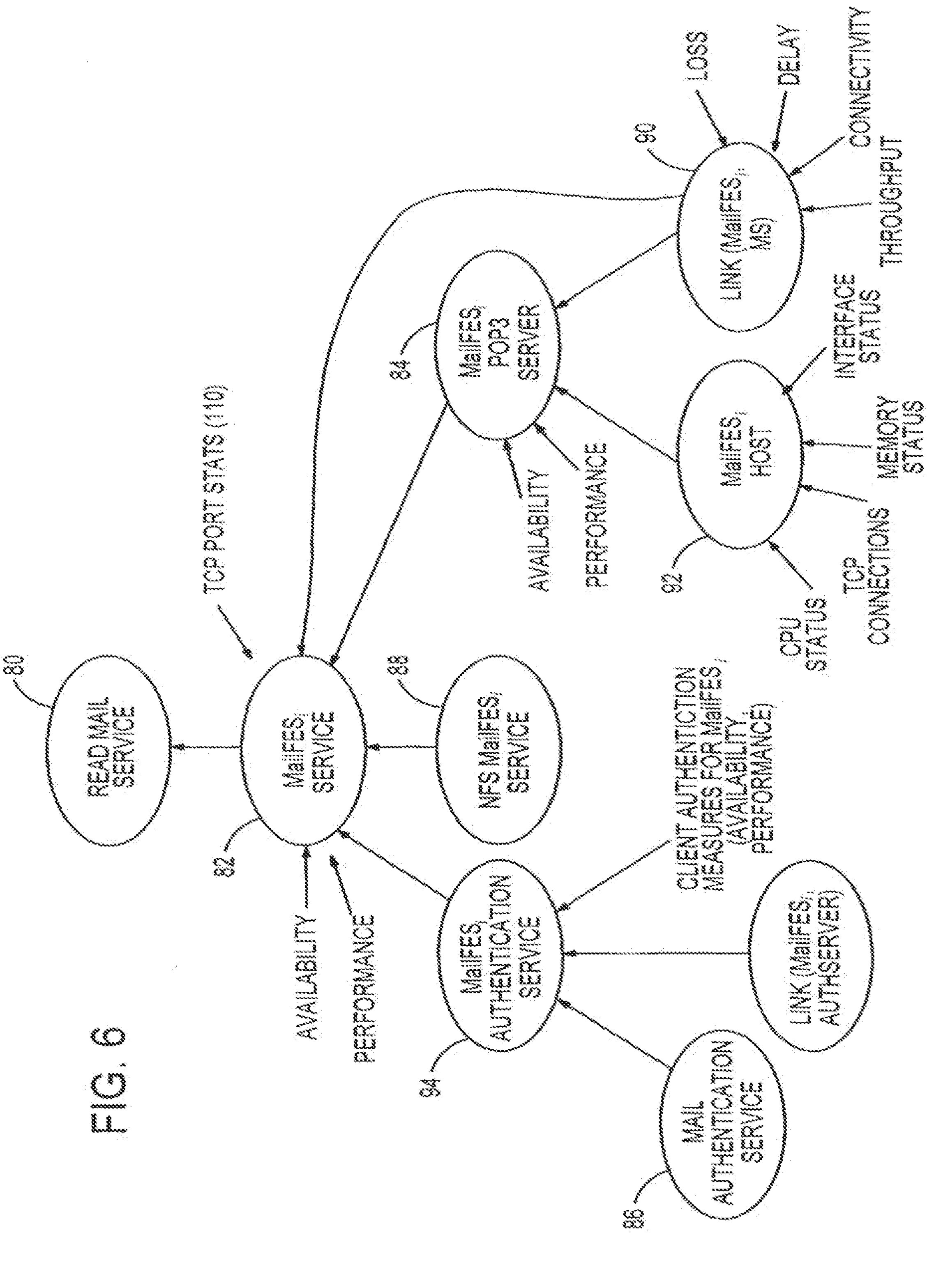

READ MAIL SERVICE
80
MailFES$_i$ SERVICE
82
TCP PORT STATS (110)
NFS MailFES$_i$ SERVICE
88
AVAILABILITY
PERFORMANCE
MailFES$_i$ AUTHENTICATION SERVICE
94
CLIENT AUTHENTICTION MEASURES FOR MailFES$_i$ (AVAILABILITY, PERFORMANCE)
LINK (MailFES$_i$, AUTHSERVER)
MAIL AUTHENTICATION SERVICE
86
MailFES$_i$ POP3 SERVER
84
AVAILABILITY
PERFORMANCE
MailFES$_i$ HOST
92
CPU STATUS
TCP CONNECTIONS
MEMORY STATUS
INTERFACE STATUS
LINK (MailFES$_i$, MS)
90
LOSS
DELAY
CONNECTIVITY
THROUGHPUT

FIG. 6

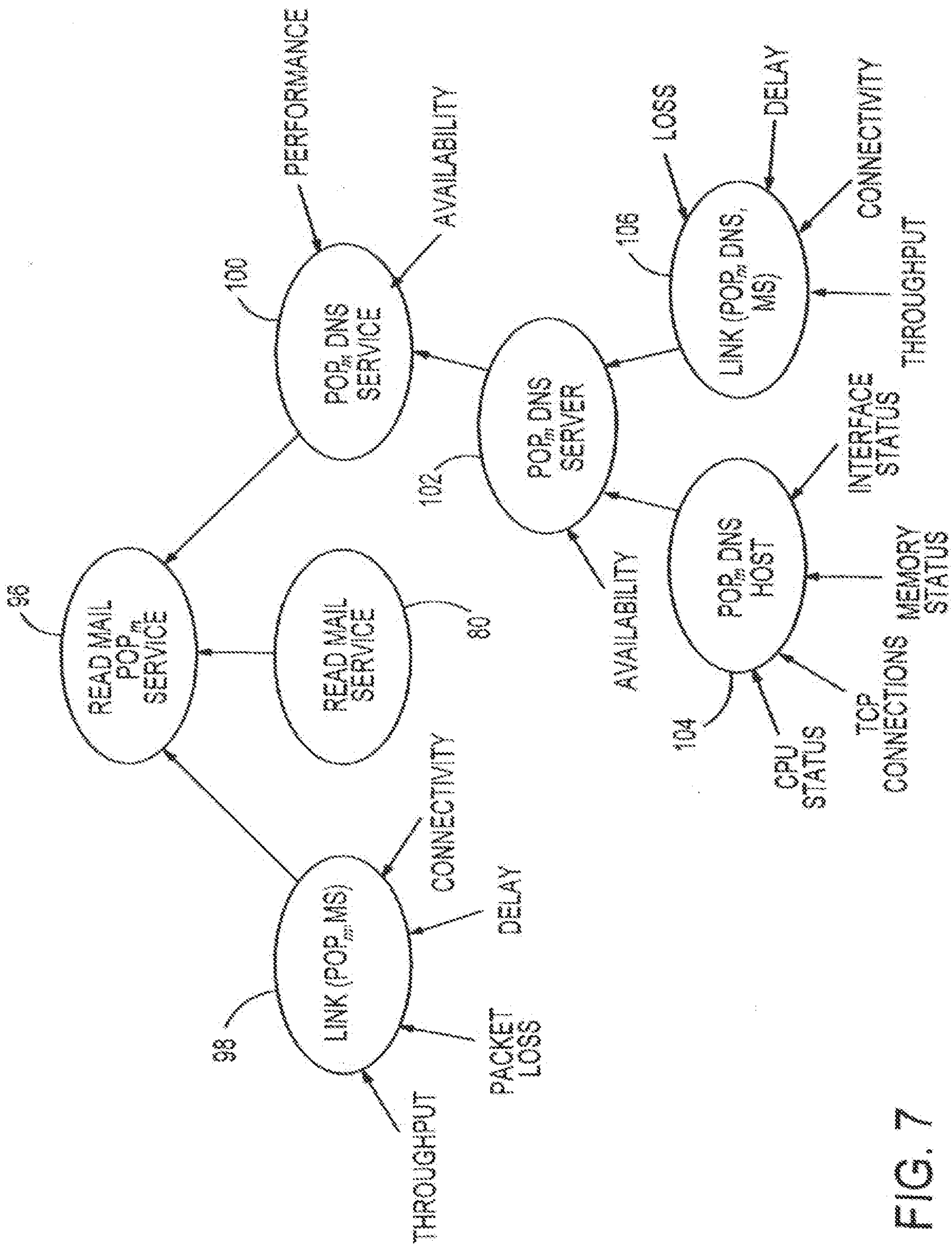

PERFORMANCE
AVAILABILITY
100
POP$_m$ DNS SERVICE
106
LOSS
DELAY
CONNECTIVITY
THROUGHPUT
LINK (POP$_m$ DNS, MS)
102
POP$_m$ DNS SERVER
INTERFACE STATUS
MEMORY STATUS
TCP CONNECTIONS
CPU STATUS
104
POP$_m$ DNS HOST
AVAILABILITY
96
READ MAIL POP$_m$ SERVICE
READ MAIL SERVICE
80
98
LINK (POP$_m$,MS)
CONNECTIVITY
DELAY
PACKET LOSS
THROUGHPUT

FIG. 7

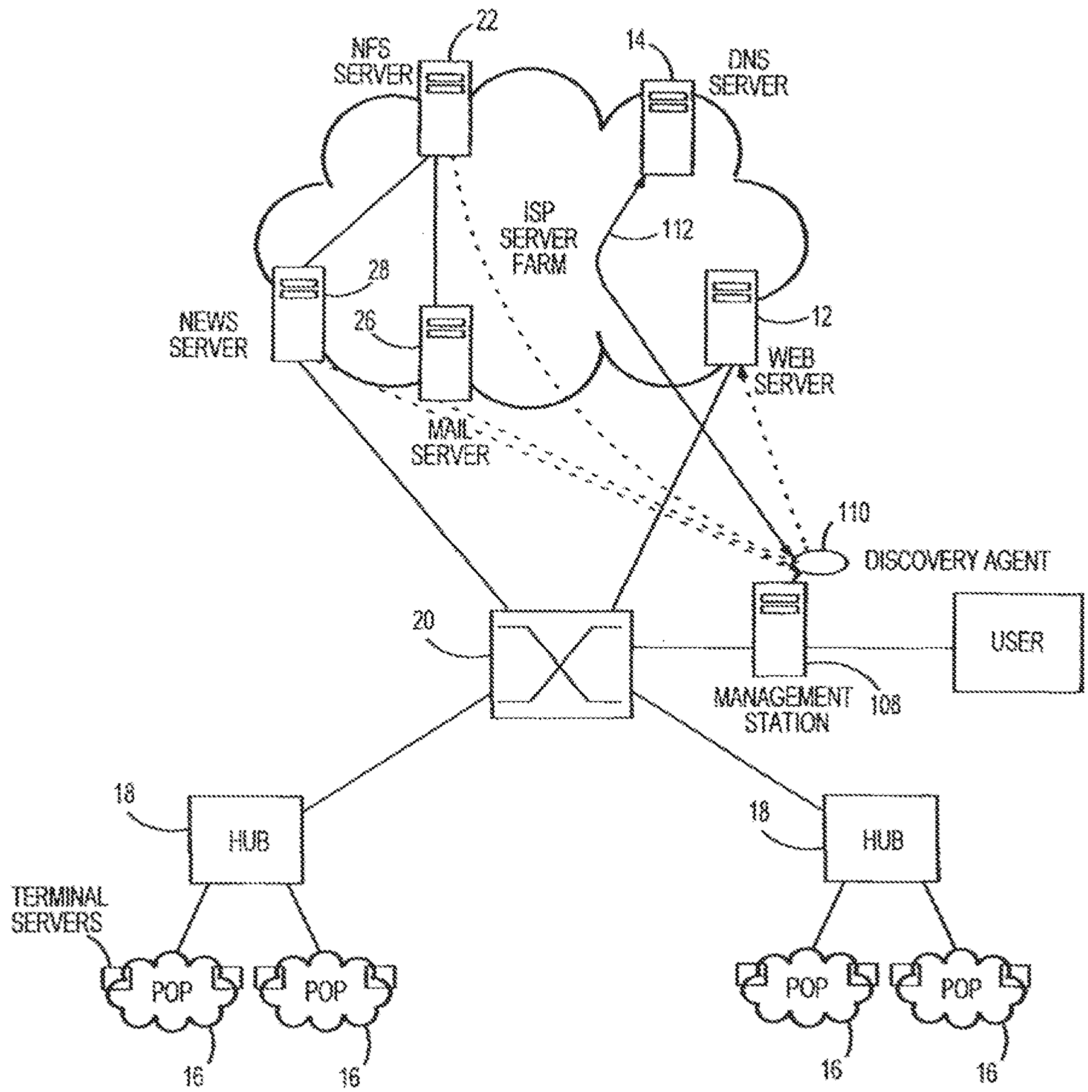

22
NFS SERVER
14
DNS SERVER
ISP SERVER FARM
112
28
NEWS SERVER
26
MAIL SERVER
12
WEB SERVER
110
DISCOVERY AGENT
20
MANAGEMENT STATION
108
USER
18
HUB
18
HUB
TERMINAL SERVERS
POP
POP
POP
POP
16
16
16
16

FIG. 8

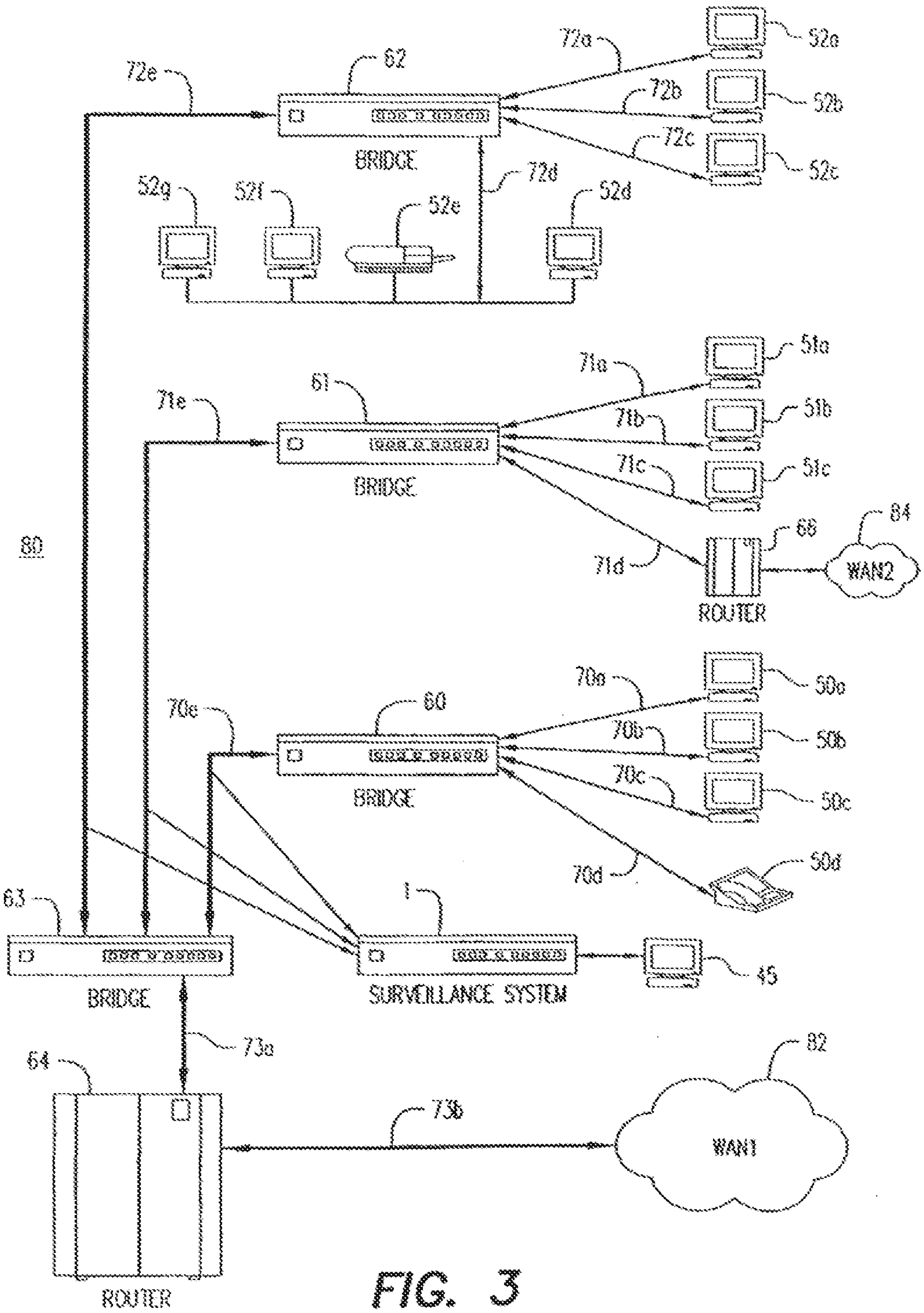

72a
52a
72e
62
72b
52b
BRIDGE
72c
52c
72d
52g
52f
52e
52d
51a
71a
61
71e
71b
51b
BRIDGE
71c
51c
84
80
68
WAN2
71d
ROUTER
70a
50a
70e
60
70b
50b
BRIDGE
70c
50c
70d
50d
63
1
BRIDGE
SURVEILLANCE SYSTEM
45
73a
82
64
73b
WAN1
ROUTER

FIG. 3

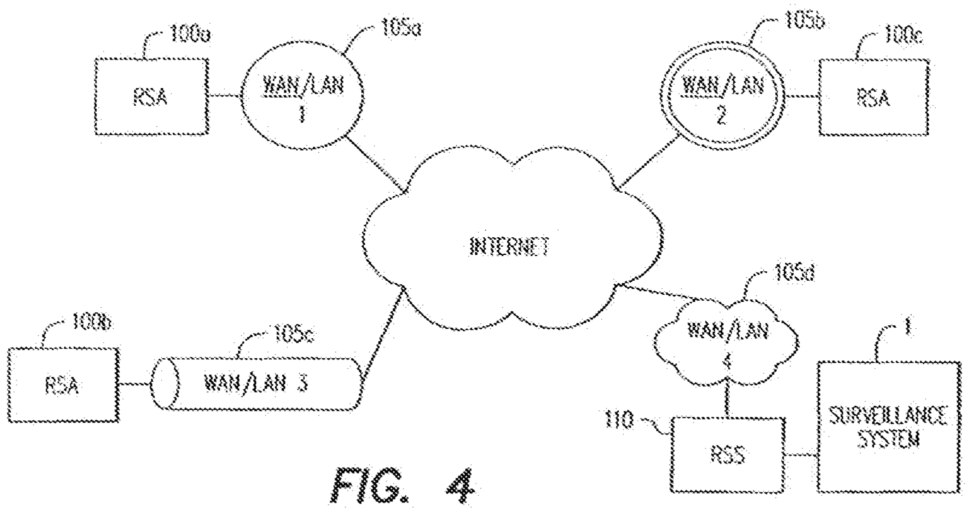

100a
RSA
105a
WAN/LAN 1
105b
WAN/LAN 2
100c
RSA
INTERNET
105d
WAN/LAN 4
1
SURVEILLANCE SYSTEM
110
RSS
100b
RSA
105c
WAN/LAN 3

FIG. 4

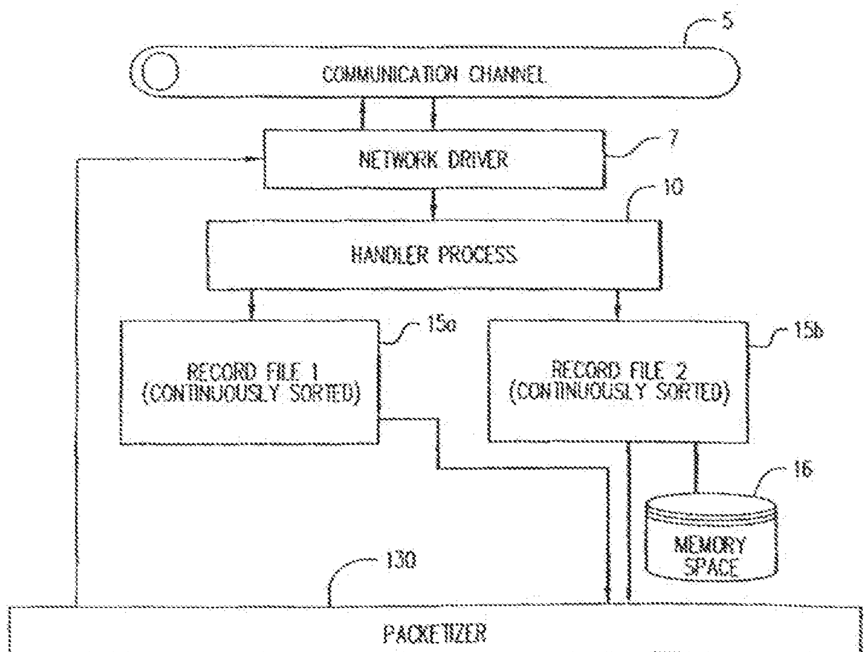

5
COMMUNICATION CHANNEL
NETWORK DRIVER
7
10
HANDLER PROCESS
15a
RECORD FILE 1 (CONTINUOUSLY SORTED)
RECORD FILE 2 (CONTINUOUSLY SORTED)
15b
16
MEMORY SPACE
130
PACKETIZER

FIG. 5

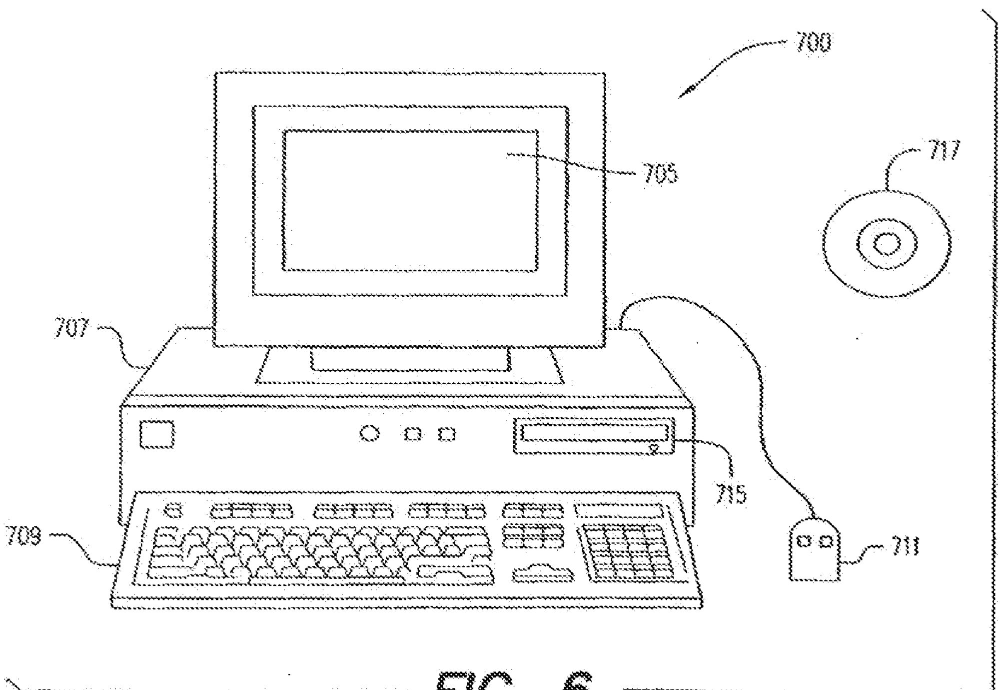


FIG. 6

METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION

COPYRIGHT NOTICE

MICROFICHE APPENDIX

A microfiche appendix including 64 frames on two fiche is included herewith.

BACKGROUND OF THE INVENTION

This invention relates to transmission of information between multiple digital devices on a network and between multiple networks on an internetwork. More particularly, this invention relates to a method and apparatus for ensuring secure network communications by conducting surveillance and checking of all or nearly all data transmitted on a network, by network session reconstruction, and by security breach intervention.

Networking Devices Standards

This specification presumes some familiarity with the general concepts, protocols, and devices currently used in LAN networking applications and in WAN internetworking applications. As these standards are widely publicly available, they will not be fully discussed here.

Generalized Lan Configuration

FIG. 3 is a generalized diagram of a local area network (LAN) 80 of a type that might be used today in a moderate-sized office or academic environment and as an example for discussion purposes of one type of network in which the present invention may be effectively employed. LANs are arrangements of various hardware and software elements that operate together to allow a number of digital devices to exchange data within the LAN and also may include internet connections to external wide area networks (WANs) such as WANs 82 and 84. Typical modern LANs such as 80 are comprised of one to many LAN intermediate systems (ISs) such as ISs 60-62 that are responsible for data transmission throughout the LAN and a number of end systems (ESs) such as ESs 50a-d, 51a-c, and 52a-g, that represent the end user equipment. The ESs may be familiar end-user data processing equipment such as personal computers, workstations, modems for dial-up connections, and printers and additionally may be digital devices such as digital telephones or real-time video displays. Different types of ESs can operate together on the same LAN. Many different LAN configurations are possible, and the invention is not limited in application to the network shown in FIG. 3.

Security problems in network communications

A problem that has increasingly arisen in LAN and WAN environments is that in most prior art networks packet traffic on the line is fundamentally insecure. LANs are often designed to provide easy and flexible access to network-wide resources to any user process connected to the LAN, including processes connected through internet or dial-up connection. Within a corporate LAN, many users may have access to computer files containing data, such as account balances or financial transaction information, that may be manipulated in order to commit or cover-up crime. Firewalls are one technology to prevent unauthorized access from outside a LAN to files on the LAN. But the vast majority of computer crime is perpetrated by authorized, inside users of the LAN, accessing or manipulating data in ways that are not authorized. Firewalls offer no protection against unauthorized insider access to LAN resources.

Other security issues involve spoofing and sniffing. In a LAN segment such as 72d, for example, every ES on the LAN segment will hear every packet sent to any ES on that segment. In general, each ES in the network has a unique ethernet (or MAC) address, and an ES will discard any packets it hears that are not addressed to its MAC address. However, ESs are not forced by the network to discard packets not addressed to them and may operate in a promiscuous mode in which the ES reads every packet it hears on the network and passes that packet up to higher layer software running in the ES. While promiscuous mode has legitimate uses during adaptor configuration or debugging, it can also be used by an ES to read and examine all the network traffic on the network without authorization. This activity is sometimes known in the art as sniffing.

A problem related to sniffing can happen during transmissions from a LAN whereby software running on the LAN can send the outgoing packet addresses to mimic another ES's packets. This technique is known in the art as spoofing. An unscrupulous user spoofing another's packets can introduce unwanted data, such as viruses, into a packet stream being transmitted from the ES, or can hijack a user's network session and gain unauthorized access to other system resources.

A number of techniques have been proposed or implemented to enhance network security. In general, all of these techniques rely on verification of either a MAC address, and IP address, or a user identification. These techniques are limited, however, because there is no guarantee that packets being transmitted on the network have a valid MAC or IP address in their packet header and there is also no guarantee that an authorized user of a LAN will not access or manipulate LAN data in an unauthorized way.

What is needed is a simple, inexpensive, system for monitoring the activity on a network and scanning for unauthorized network activity and automatically taking action when unauthorized activity is detected. Ideally, such a technique should be implementable on a network without decreasing network performance.

For purposes of clarity, the present discussion refers to network devices and concepts in terms of specific examples. However, the method and apparatus of the present invention may operate with a wide variety of types of network devices including networks dramatically different from the specific examples illustrated in FIG. 3 and described below. It is therefore not intended that the invention be limited except as done so in the attached claims.

In many existing LAN systems, data on the network is grouped into discrete units referred to as packets, each having an indication of source and destination. While the present invention is not limited to packetized data, data is described herein in terms of packets in order to ease understanding.

SUMMARY OF THE INVENTION

The invention is an improved method and apparatus for transmitting data in a LAN. According to the present invention, a Network Security Agent™ surveillance system, is able to read all packets transmitted on a network segment, reconstruct all user sessions, and scan all user sessions for noteworthy or suspicious activity, all in real-time and without any significant impact on network performance. When any noteworthy or suspicious activity is detected, alerts are generated and appropriate intervention actions can be taken.

The present invention makes use of Packet Sniffing, Session Reconstruction, and Session Scanning in order to scan sessions for unauthorized activity and, when unauthorized activity is detected, predetermined automatic intervention action is taken. The present invention uses automatic real-time session reconstruction and scanning to accomplish network surveillance on the tens of millions of packets generated on a typical LAN each day.

In accordance with the present invention, hardware and software elements are optimally designed to be able to read all packets on the LAN in real-time and reconstruct sessions. Customized routines for reading low-level packets directly from the ethernet controller are incorporated in the invention in order to capture 100% of all network traffic.

In one embodiment, the invention includes software elements written in a language optimized for data handling and I/O. The invention includes a set of user interfaces to allow a network administrator to review data gathered by the invention and to set certain parameters.

The invention will be better understood with reference to the following drawings and detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a network surveillance system according to the present invention.

FIG. 2 is a block diagram of a handler process in accordance with an embodiment of the invention.

FIG. 3 is a diagram of a generalized LAN in which the present invention may be employed.

FIG. 4 illustrates a number of remote networks with remote surveillance system agents according to an embodiment of the invention.

FIG. 5 illustrates a remote surveillance system agent according to an embodiment of the invention.

FIG. 6 is a block diagram of a computer system which may be configured with a software embodiment in accordance with the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Overview

FIG. 1 is a block diagram of a network surveillance system in accordance with one embodiment of the present invention. Shown in FIG. 1 is a communication channel 5 which indicates a connection to a LAN or other data communication medium. Data, either packetized or otherwise, is received from channel 5 by a network driver 7 which may include hardware and software components for quickly reading the signals on channel 5 and translating them into computer readable data. Network driver 7 may be a preexisting or custom network interface and is set to be in promiscuous mode in which it receives all or nearly all data transmitted on channel 5. Data received on network driver 7 are passed to handler process 10, which may preform some filtering or processing of the data as described below, before placing the data as records into one of files 15*a* or 15*b* as described below. Files 15*a* and 15*b* are continuously sorted as is known in the art. Scanner process 30 reads records from files 15*a*–*b* and organizes the records into a session database 32. Session data base 32 contains a sequential listing of all packets received in a particular session. According to the invention, scanner process 30 includes a session window (SW) scanner 34. SW scanner 34 defines session windows for reading windows of data in session data base 32 and testing a set of rules 38 against those windows of data.

According to the invention, session windows are constructed so as to provide an overlapping and sliding window of data so that rules may be fully tested even if the data that would fire the rule is split on packet reception between record file 1 and record file 2. Data bases 40*a*–*d* are maintained to provide information regarding network usage parameters such as accessed URLs, accessed domains, the top ten URLs accessed, etc. A user interface 42 is designed to accept user instructions from a work station such as 45 and to display requested data to the work station 45 as described below. An optional real time display engine 44 may interact with handler process 10 to display real-time session data.

According to the invention, newly transmitted packets on channel 5 are captured even while previously captured packets are being scanned by incorporating two record files 15*a* and 15*b* which operate such that while a record file is being scanned and analyzed for surveillance incidents, the other record file is being filled with continuously sorted packets by handler process 10. Associated with the record files also may be a memory space 16 for storing larger amounts of packet data.

Handler Process

FIG. 2 illustrates the functions of handler process 10 according to one embodiment of the invention. Handler 10 reads all or a large subset of data on channel 5 and selects session packets for later reconstruction. Handler 10 communicates with scanner 30 and real time display engine 44.

Handler 10 prioritizes reading packets from channel 5, which on a busy LAN can be in excess of 50,000,000 packets a day. One embodiment of the handler uses a small state-table and is completely event driven. Reading data from network 5 packets takes the highest priority so that no desired packets are missed.

Handler process 10 includes a filtering process 22 for initial packet filtering. Filtering process 22 can be set, according to the invention, to filter out packets based on a number of criteria including filtering out invalid packets due to a bad check sum or certain identifications.

Handler process 10 also includes a timestamper 23 for adding a time stamp to each network packet received and a sequencer 25 for adding a sequence number to each packet received in order to uniquely identify each packet. Handler decodes 26 partially decodes network packets and can be programmed to handle certain internal packet compression.

Recorder 28 writes each processed data packet out as a record into a continuously sorted record files 15*a*–15*b*. Which file is written to is determined scanner process 30, as described below. A representative record 18 is shown in FIG. 1 having a number of fields including indications for a source, a destination or group of destinations, a server, a sequence number, data, a timestamp (T.S.), and a handle sequence number (HSQ).

Scanner Process

Scanner 30's primary task is session reconstruction and session scanning. At timed intervals, scanner 30 sets a flag requesting a group of packets for session reconstruction. The packets are generally provided by handler 10 from either file 15*a* or 15*b* and handler 10 begins storing newly received records in the file not being accessed by scanner 30. When scanner 30 receives the packets, it immediately proceeds to reconstruct sessions.

Sessions are reconstructed based on any combination of source and destination indications such as IP address and port (for TCP/IP) or Local Area Transport (LAT) virtual circuit and slot. Each identified session is reconstructed separately along with a session identifier. Some portion of previously reconstructed session data is maintained to allow SW scanner 34 to detect patterns that may cross record files.

Rules and Intervention Actions

The reconstructed session is passed through a series of user-defined rules 38. In one embodiment, each rule consists of simply an alert name and a pattern. When SW scanner 34 detects that a session window contains the pattern, the alert is triggered.

Associated with each alert name is a description of the alert, a list of actions to be taken when the alert is triggered, and the priority level of the alert. When the alert is triggered, an incident is logged in log 39. Incident log 39 contains identifying data of the incident such as the name of the alert, description, user login name, location (TCP/IP or LAT address/port), and a snapshot of the session-with an arrow pointing to the pattern that caused the alert to be triggered.

After logging the incident, any alert actions are taken by alert handler 36. Possible alert actions include sending email to someone or group of people containing for example the name of the triggered alert, location (TCP/IP or LAT address/port), user login name, and a snapshot of the session with an indication of the pattern that caused the alert to be triggered.

Another possible alert action includes recording the session from the alert moment forward for playback later on. The recording contains, keystroke-for-keystroke, everything that the user does that involves transmission over the network. An alert may also take action to terminate the user connection that generated it.

Scanner 30 also may handle session data base cleanup procedures—such as purging inactive login information.

Real Time Display Module

Real time display module 44 is an optional component of the invention that is in charge of displaying sessions in real-time. When real time display module 44 receives a watch message from either alert handler 36 or user interface module 42, it creates a terminal-emulation pop-up window. Each window displays a user session in real time keystroke by keystroke. In this situation, both scanner 30 and real time display module 44 will receive certain packets from handler 10. Real time display module 44 then sends a message to handler 10, requesting that packets from the watched session be duplicated and sent to real time display module 44. When watch packets are received, they are formatted and sent to the appropriate terminal-emulation pop-up window.

If the session is disconnected, a session closed message is displayed in the pop-up window and watching of the session is halted. If the user manually closes the pop-up window, session watching is also discontinued for that session.

User Interface Module

User interface module 42 provides a user interface to the network surveillance system. From module 42, sessions can be viewed, reports generated, alerts and rules defined, and session actions taken.

Module 42 communicates with real time display module 44 when session watching is requested. All other displays and actions performed by module 42 are performed through data base operations. Scanner 30 notices data base changes (such as new alerts or rules) and rebuilds its internal tables as needed.

Module 42 can be operated either with a mouse, directly from the keyboard, or by any other method for interfacing between a computer work station and a user. Extensive on-line help is provided at all decision points.

EXAMPLE

The operation of the invention may be further understood by an example. For the purposes of this example, assume that LAN 80 is a local area network in an investment management firm. The network may include a number of functions which a particular employee is authorized to use at any time from any location, including from a dial-up connection. One such function that an employee may access at any time is interoffice email functions. In addition, the LAN may include data of a sensitive nature pertaining to customer accounts, which normally would only be accessed by authorized employees during business hours while on-site at the office handling customer accounts. Standard prior art security measures, such as file access authorization, might designate certain employees to have access to this data, but would usually not limit that access based on whether the employee was connecting via a dial-up connection or whether the employee was attempting to access the data during valid business hours.

According to the current invention, a rule could be set up to monitor access to any file within the customer file structure. This rule could be a very simple rule that checked for a certain text string being passed from a client process to a server process over the network where that text string represented a file path name. To further illustrate aspects of the invention, assume that the complete file path name is divided into more than one network packet and that the two network packets are received just as scanner 30 requests a switch from record file 1 to record file 2.

Such a rule may be represented as:

```
IF          text_contains("\datacustomer") AND
            (time()=off_hours OR connection()=dial_up)
THEN
            email(session_data, supervisor)
            terminate_session ()
ENDIF
```

According to this example, a first packet from a session S2 ending with the data "\data\cu" is transmitted on channel 5 and placed by handler 10 into record file 15a, before the next packet from S2 is received, scanner 30 signals to handler 10 to switch record files. Scanner 30 then reads the data in record file 1, and places data from S2 in the appropriate session database file. Session window scanner 34 then scans the text in SW2 for the above rule, and since the text is not found, the rule does not fire.

In the meantime, a second packet from session S2 beginning with the data "stomer" is transmitted on channel 5 and placed by handler 10 into record file 15b. When scanner 30 has fully analyzed the data from 15a, it switches to 15b and places the additional data from S2 in the appropriate session database file. Session window scanner 34 then scans the text in SW2 for the above rule, and, because SW2 includes an overlap of at least 13 bytes, the rule fires. The incident is logged in 39 and the alert is handled by handler 36.

Specific Implementation

A primary challenge of the present invention is to be able to read all data packets on the LAN in real-time. In one specific installation, an OpenVMS operating system, running on a Digital Alpha/AXP CPU at speeds of 233 Mhz to 500 Mhz was chosen to keep up with the heavy processing demands of reading 100% of a busy LAN's packets while handling session reconstruction, real-time scanning, and real-time display tasks.

Customized routines for reading low-level packets directly from a network controller were written in C using the OpenVMS' asynchronous QIO services. The real-time display module was also written in C.

For session reconstruction and real-time session scanning, one embodiment was implemented using the INTOUCH 4GL(TM) programming language, developed by the assignee of the present invention. INTOUCH 4GL is a high performance language designed specifically for data manipulation and text scanning. For use by the surveillance agent INTOUCH 4GL was enhanced by including specialized functions for high-speed pattern matching.

INTOUCH 4GL was also used for the user interface and incident tracking, reporting, data base maintenance, and recorded session playback.

Remote Surveillance Agent

FIGS. 4 and 5 illustrate a different embodiment of the invention wherein a number of remote surveillance agents (RSAs) may be utilized along with an internet in order to capture network data traffic on one site and have that traffic analyzed and sessions reconstructed at another site. FIG. 4 shows RSAs **100a–c** connected to different WAN/LAN networks **105a**. According to this embodiment, RSAs **100a–c** collect all network data traffic from the LAN or WAN to which they are attached, but instead of fully scanning that traffic, RSAs **100a–c** store collected packets into a form that may be transmitted to remote surveillance server (RSS) **110**. RSS **110** receives the information for RSAs **100a–c** and presents this information to a surveillance system **1** according to the invention, which performs session reconstruction, rule checking, and alert handling as described above.

According to one specific embodiment RSAs **100a–c** collect multiple packets on their attached WAN/LAN and compress multiple packets into a single internet packet which may be transmitted back through the WAN/LAN, over the internet, to RSS **110**. According to this embodiment, RSAs **100a–c** can in this way allow a surveillance system **1** located in one city to monitor several WAN/LANs located in different cities simply by plugging an RSA into the remote network without making any other changes to the network.

FIG. 5 illustrates one example of an RSA according to the invention. LAN/WAN data is received and processed by handler process **10** substantially as described above and stored in one of a plurality of record files **15a–b**. Record file data is then read by internet packetized **130**, which stores multiple LAN/WAN packets into an internet packet which is then passed to driver **7** for transmission to RSS **110** via the internet. In an alternative embodiment, LAN/WAN packets are received by an RSA and timestamped and immediately transmitted over the internet, either singly or in groups, with minimal additional processing by the RSA.

The present invention may be embodied in software instructions either recorded on a fixed media or transmitted electronically. In such a case, the surveillance system **1** of FIG. 3 will be a high performance computer system and the software instructions will cause the memory and other storage medium of computer **1** to be configured as shown in FIG. 1 and will cause the processor of computer **1** to operate in accordance with the invention.

FIG. 6 illustrates an example of a computer system used to execute the software of the present invention. FIG. 7 shows a computer system **700** which includes a monitor **705**, cabinet **707**, keyboard **709**, and mouse **711**. Cabinet **707** houses a disk drive **715** for reading a CD-ROM or other type disk **717** and houses other familiar computer components (not shown) such as a processor, memory, disk drives, and the like, as well as an adaptor **1** for connection to a communication channel **5**.

The invention has now been explained with reference to specific embodiments. Other embodiments will be apparent to those of skill in the art. In particular, specific processing orders have been described and functions have been described as being in particular orders, however, many of these sub functions could be differently arranged without changing the essential operation of the invention. It is therefore not intended that this invention be limited, except as indicated by the appended claims.

What is claimed is:

1. A network surveillance system for conducting surveillance on a network independent of a network server comprises:

a network driver for capturing data on a network, said data not necessarily addressed to said surveillance system;

a handler process for receiving data from said network driver and storing said data in real time;

a plurality of record files for receiving network data and storing said data before further examination;

a scanner process for designating one of said plurality of record files as a receive file while reading data from another of said plurality of record files and for using said data to construct a plurality of session data streams, said session data streams providing a sequential reconstruction of network data traffic organized by session;

a session window scanner for reading a window of data in one of said plurality of session data streams;

a set of surveillance rules defining data patterns which, when met, will trigger a surveillance alert; and

an alerts handler for responding to fired rules and taking defined actions.

2. The device according to claim 1 further comprising:

a user interface allowing a user to view sessions in real time and to access a plurality of data bases containing session events maintained by said scanner process.

3. The device according to claim 1 wherein said handler process filters certain network data and adds an indication of the time when certain network data is received from the network.

4. The device according to claim 1 wherein said plurality of record files are continuously sorted according to a record index.

5. The device according to claim 1 wherein said session window includes an overlap portion of previously examined data from said session data base in order to test for rules that would apply to data contained in more than one record.

6. The device according to claim 5 wherein said session window overlap is determined by the longest text string that could trigger a rule.

7. The device according to claim 1 wherein said alerts handler may respond to an alert by transmitting a message to a specified plurality of destinations.

8. The device according to claim 1 wherein said alerts handler may respond to an alert by forcing a user session to terminate.

9. The device according to claim 1 wherein said alerts handler may respond to an alert by recording a session.

10. A fixed computer readable medium containing computer executable program code, which, when loaded into an appropriately configured computer system will cause the computer to embodiment the device of claim 1.

11. A method for for conducting surveillance on a network comprises:

capturing data on a network;

storing said data in real time in one of a plurality of record files;

using said data to construct a plurality of session data streams, said session data streams providing a sequential reconstruction of network data traffic organized by session;

reading a window of data in one of said plurality of session data streams;

testing said window of data against a set of surveillance rules; and

responding to fired rules by taking defined interventions.

12. The method according to claim 11 further comprising presenting a view of reconstructed sessions to a user in real time.

13. The method according to claim 11 further comprising filtering certain network data packets before storing.

14. The method according to claim 11 further comprising continuously sorting record files.

15. The method according to claim 11 further comprising examining an overlap portion of previously examined data in order to test rules that would apply to data contained in more than one record.

16. The method according to claim 15 wherein said session window overlap is determined by the longest text string that could trigger a rule.

17. The method according to claim 11 further comprising responding to an alert by transmitting a message to a specified plurality of destinations.

18. The method according to claim 11 further comprising responding to an alert by forcing a user session to terminate.

19. The method according to claim 11 further comprising responding to an alert by recording a session.

20. A fixed computer readable medium containing computer executable program code, which, when loaded into an appropriately configured computer system will cause the computer to embodiment the method of claim 11.

* * * * *

Linux FreeS/WAN Index file

This is an index file for the Linux FreeS/WAN documentation. Most files described here are in the doc directory after the distribution is unpacked and are in HTML format. If you prefer text files over HTML, see doc/README for instructions on creating them.

Files most users should read

- How to set up a simple network with FreeS/WAN. This also covers initial installation.
- Configuration of FreeS/WAN.
- relation between IPSEC and firewalls
- a list of FreeS/WAN man pages with links to HTML versions.
  They are also of course available via the *man* command.
- information on the project mailing list
- problem reporting
- Troubleshooting using our ipsec_barf(8) and ipsec_look(8) tools and other tools such as tcpdump (8) and sniffers
- a (still rudimentary) FAQ document

Distribution text files

Text files in the main distribution directory are README, INSTALL, CREDITS, CHANGES, and COPYING.

License and copyright information

All code and documentation written for this project is distributed under either the GNU General Public License (GPL) or the GNU Library General Public License. For details see COPYING.

Not all code in the distribution is ours, however. See CREDITS for details. In particular, note that the Libdes library has its own license

Printed documentation

Those who prefer documentation in printed form can, of course, print any of the HTML documents or man pages in the usual way, and are free to write whatever scripts they like to reformat them in the process. (We would like to see any interesting scripts you come up with. Please post them, or a suitable pointer, to the mailing list. Of course, if they have any code specifically related to cryptography, you must consult your local export laws first.)

We also provide three files designing for use with the "make book" command in the Amaya web browser/editor from the World Wide Web Consortium.

Going to any of these files with Amaya and clicking on the "make book" command will give you one large file, with an automatically generated table of contents, for browsing or printing:

- Setup, configuration, troubleshooting

- Background information
- Man pages

These files are also usable without Amaya. Without Amaya, you cannot build the single large "book" file, but you can follow the links to its components.

Project background information

- Our project leader's rationale for starting this
- Project Overview: goals, protocols, and components
- Lists of IPSEC features
  - implemented in Linux FreeS/WAN
  - not yet in Linux FreeS/WAN
- DES and its vulnerability to cracking.
- Export laws

Reference information

Automatically generated link files

- Table of Contents for HTML documentation
- Permuted index of HTML files

Run 'make' in the doc directory if these files aren't there.

Other reference files

- Roadmap, where things are in the distribution
- Glossary of terms and acronyms
- Bibliography
- Web links for
  - Linux FreeS/WAN project
  - IPSEC protocols
  - Linux
  - Cryptography and security
- Mailing lists
- List of IPSEC and other security RFCs

Specialised information

- Troubleshooting using our ipsec_barf(8) and ipsec_look(8) tools and other tools such as tcpdump (8) and sniffers
- Compatibility information culled from the mailing list on using FreeS/WAN with:
  - Linux distibutions other than Redhat
  - CPUs other than Intel architecture
  - other IPSEC implementations
- Configuration for setups with unusual requirements such as:
  - extruded subnet (IP sees one network, but there are two or more physical sites involved).

  - Road Warrior support
  - dynamic interface (not up at boot time, e.g. PCMCIA) handling
- implementation notes on various topics
- cross-reference between various standards and the FreeS/WAN code and utilities

This file is part of the documentation for the Linux FreeS/WAN project.
See the documentation index or project home page for more information.

Swan: Securing the Internet against Wiretapping by project founder John Gilmore

My project for 1996 was to **secure 5% of the Internet traffic against passive wiretapping**. It didn't happen in 1996, so I'm still working on it in 1997, 1998, and 1999! If we get 5% in 1999 or 2000, we can secure 20% the next year, against both active and passive attacks; and 80% the following year. Soon the whole Internet will be private and secure. The project is called S/WAN or S/Wan or Swan for Secure Wide Area Network; since it's free software, we call it FreeSwan to distinguish it from various commercial implementations. RSA came up with the term "S/WAN". Our main web site is at http://www.xs4all.nl/~freeswan/. Want to help?

The idea is to deploy PC-based boxes that will sit between your local area network and the Internet (near your firewall or router) which opportunistically encrypt your Internet packets. Whenever you talk to a machine (like a Web site) that doesn't support encryption, your traffic goes out "in the clear" as usual. Whenever you connect to a machine that does support this kind of encryption, this box automatically encrypts all your packets, and decrypts the ones that come in. In effect, each packet gets put into an "envelope" on one side of the net, and removed from the envelope when it reaches its destination. This works for all kinds of Internet traffic, including Web access, Telnet, FTP, email, IRC, Usenet, etc.

The encryption boxes are standard PC's that use freely available Linux software that you can download over the Internet or install from a cheap CDROM.

This wasn't just my idea; lots of people have been working on it for years. The encryption protocols for these boxes are called IPSEC (IP Security). They have been developed by the IP Security Working Group of the Internet Engineering Task Force, and will be a standard part of the next major version of the Internet protocols (IPv6). For today's (IP version 4) Internet, they are an option.

The Internet Architecture Board and Internet Engineering Steering Group have taken a strong stand that the Internet should use powerful encryption to provide security and privacy. I think these protocols are the best chance to do that, because they can be deployed very easily, without changing your hardware or software or retraining your users. They offer the best security we know how to build, using the Triple-DES, RSA, and Diffie-Hellman algorithms.

This "opportunistic encryption box" offers the "fax effect". As each person installs one for their own use, it becomes more valuable for their neighbors to install one too, because there's one more person to use it with. The software automatically notices each newly installed box, and doesn't require a network administrator to reconfigure it. Instead of "virtual private networks" we have a "REAL private network"; we add privacy to the real network instead of layering a manually-maintained virtual network on top of an insecure Internet.

Deployment of IPSEC

The US government would like to control the deployment of IP Security with its crypto export laws. This isn't a problem for my effort, because the cryptographic work is happening outside the United States. A foreign philanthropist, and others, have donated the resources required to add these protocols to the Linux operating system. Linux is a complete, freely available operating system for IBM PC's and several kinds of workstation, which is compatible with Unix. It was written by Linus Torvalds, and is still maintained by a talented team of expert programmers working all over the world and coordinating over the Internet. Linux is distributed under the GNU Public License, which gives everyone the right to copy it, improve it, give it to their friends, sell it commercially, or do just about anything else with it, without paying anyone for the privilege.

Organizations that want to secure their network will be able to put two Ethernet cards into an IBM PC, install Linux on it from a $30 CDROM or by downloading it over the net, and plug it in between their Ethernet and their Internet link or firewall. That's all they'll have to do to encrypt their Internet traffic everywhere outside their own local area network.

Travelers will be able to run Linux on their laptops, to secure their connection back to their home network (and to everywhere else that they connect to, such as customer sites). Anyone who runs Linux on a standalone PC will also be able to secure their network connections, without changing their application software or how they operate their computer from day to day.

There will also be numerous commercially available firewalls that use this technology. RSA Data Security is coordinating the S/Wan (Secure Wide Area Network) project among more than a dozen vendors who use these protocols. There's a compatability chart that shows which vendors have tested their boxes against which other vendors to guarantee interoperatility.

Eventually it will also move into the operating systems and networking protocol stacks of major vendors. This will probably take longer, because those vendors will have to figure out what they want to do about the export controls.

Current status

My initial goal of securing 5% of the net by Christmas '96 was not met. It was an ambitious goal, and inspired me and others to work hard, but was ultimately too ambitious. The protocols were in an early stage of development, and needed a lot more protocol design before they could be implemented. As of April 1999, we have released version 1.0 of the software (freeswan-1.0.tar.gz), which is suitable for setting up Virtual Private Networks using shared secrets for authentication. It does not yet do opportunistic encryption, or use DNSSEC for authentication; those features are coming in a future release.

Protocols

> The low-level encrypted packet formats are defined. The system for publishing keys and providing secure domain name service is defined. The IP Security working group has settled on an NSA-sponsored protocol for key agreement (called ISAKMP/Oakley), but it is still being worked on, as the protocol and its documentation is too complex and incomplete. There are prototype implementations of ISAKMP. The protocol is not yet defined to enable opportunistic encryption or the use of DNSSEC keys.

Linux Implementation

> The Linux implementation has reached its first major release and is ready for production use in manually-configured networks, using Linux kernel version 2.0.36.

Domain Name System Security

There is now a release of BIND 8.2 that includes most DNS Security features.

The first prototype implementation of Domain Name System Security was funded by DARPA as part of their Information Survivability program. Trusted Information Systems wrote a modified version of BIND, the widely-used Berkeley implementation of the Domain Name System.

TIS, ISC, and I merged the prototype into the standard version of BIND. The first production version that supports KEY and SIG records is **bind-4.9.5**. This or any later version of BIND will do for publishing keys. It is available from the Internet Software Consortium. This version of BIND is not export-controlled since it does not contain any cryptography. Later releases starting with BIND 8.2 include cryptography for authenticating DNS records, which is also exportable. Better documentation is needed.

Why?

Because I can. I have made enough money from several successful startup companies, that for a while I don't have to work to support myself. I spend my energies and money creating the kind of world that I'd like to live in and that I'd like my (future) kids to live in. Keeping and improving on the civil rights we have in the United States, as we move more of our lives into cyberspace, is a particular goal of mine.

What You Can Do

Install the latest BIND at your site.

You won't be able to publish any keys for your domain, until you have upgraded your copy of BIND. The thing you really need from it is the new version of *named*, the Name Daemon, which knows about the new KEY and SIG record types. So, download it from the Internet Software Consortium and install it on your name server machine (or get your system administrator, or Internet Service Provider, to install it). Both your primary DNS site and all of your secondary DNS sites will need the new release before you will be able to publish your keys. You can tell which sites this is by running the Unix command "dig MYDOMAIN ns" and seeing which sites are mentioned in your NS (name server) records.

Set up a Linux system and run a 2.0.x kernel on it

Get a machine running Linux (say the 5.2 release from Red Hat). Give the machine two Ethernet cards.

Install the Linux IPSEC (Freeswan) software

If you're an experienced sysadmin or Linux hacker, install the freeswan-1.0 release, or any later release or snapshot. These releases do NOT provide automated "opportunistic" operation; they must be manually configured for each site you wish to encrypt with.

Get on the linux-ipsec mailing list

The discussion forum for people working on the project, and testing the code and documentation, is: linux-ipsec@clinet.fi. To join this mailing list, send email to linux-ipsec-REQUEST@clinet.fi containing a line of text that says "subscribe linux-ipsec". (You can later get off the mailing list the same way -- just send "unsubscribe linux-ipsec").

Check back at this web page every once in a while

I update this page periodically, and there may be new information in it that you haven't seen. My intent is to send email to the mailing list when I update the page in any significant way, so subscribing to the list is an alternative.

Would you like to help? I can use people who are willing to write documentation, install early releases for testing, write cryptographic code outside the United States, sell pre-packaged software or systems including this technology, and teach classes for network administrators who want to install this technology. To offer to help, send me email at gnu@toad.com. Tell me what country you live in and what your citizenship is (it matters due to the export control laws; personally I don't care). Include a copy of your resume and the URL of your home page. Describe what you'd like to do for the project, and what you're uniquely qualified for. Mention what other volunteer projects you've been involved in (and how they worked out). Helping out will require that you be able to commit to doing particular things, meet your commitments, and be responsive by email. Volunteer projects just don't work without those things.

Related projects

IPSEC for NetBSD
: This prototype implementation of the IP Security protocols is for another free operating system. Download BSDipsec.tar.gz.

IPSEC for OpenBSD
: This prototype implementation of the IP Security protocols is for yet another free operating system. It is directly integrated into the OS release, since the OS is maintained in Canada, which has freedom of speech in software.

---

gnu@toad.com, *gnu@eff.org*, *my home page*
An equal opportunistic encryptor.

This file is part of the documentation for the Linux FreeS/WAN project.
See the documentation index or project home page for more information.

Glossary for the Linux FreeS/WAN project

Entries are in alphabetical order. Some entries are only one line or one paragraph long. Others run to several paragraphs. I have tried to put the essential information in the first paragraph so you can skip the other paragraphs if that seems appropriate.

Jump to a letter in the glossary

numeric A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Other glossaries

Other glossaries which overlap this one include:

- glossary portion of the Cryptography FAQ
- an extensive crytographic glossary on Terry Ritter's page.
- The NSA's glossary of computer security on the SANS Institute site.
- an Internet Draft Crypto Glossary
- the IETF provide a glossary of Internet terms as RFC 1983
- a small glossary for Internet Security at PC magazine
- The glossary from Richard Smith's book Internet Cryptography

More general glossary or dictionary information:

- Free Online Dictionary of Computing (FOLDOC)
  - North America
  - Europe
  - Japan

  There are many more mirrors of this dictionary.
- CRC dictionary of Computer Science
- The Jargon File, the definitive resource for hacker slang and folklore
  - North America
  - Holland
  - home page

  There are also many mirrors of this. See the home page for a list.
- A general technology glossary
- An online dictionary resource page with pointers to many dictionaries for many languages
- A search engine that accesses several hundred online dictionaries
- O'Reilly Dictionary of PC Hardware and Data Communications Terms

Definitions

3DES (Triple DES)

Using three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass. The three-key version of 3DES is the default encryption algorithm for Linux FreeS/WAN.

IPSEC always does 3DES with three different keys, as required by RFC 2451. For an explanation of the two-key variant, see two key triple DES. Both use an EDE encrypt-decrypt-encrpyt sequence of operations.

Single DES is insecure.

Double DES is ineffective. Using two 56-bit keys, one might expect an attacker to have to do 2^{112} work to break it. In fact, only 2^{57} work is required with a meet-in-the-middle attack, though a large amount of memory is also required. Triple DES is vulnerable to a similar attack, but that just reduces the work factor from the 2^{168} one might expect to 2^{112}. That provides adequate protection against brute force attacks, and no better attack is known.

3DES can be somewhat slow compared to other ciphers. It requires three DES encryptions per block. DES was designed for hardware implementation and includes some operations which are difficult in software. However, the speed we get is quite acceptable for many uses. See benchmarks below for details.

Active attack

An attack in which the attacker does not merely eavesdrop (see passive attack) but takes action to change, delete, reroute, add, forge or divert data. Perhaps the best-known active attack is man-in-the-middle. In general, authentication is a useful defense against active attacks.

AES

The Advanced Encryption Standard, a new block cipher standard to replace DES being developed by NIST, the US National Institute of Standards and Technology. DES used 64-bit blocks and a 56-bit key. AES ciphers use a 128-bit block and are required to support 128, 192 and 256-bit keys. Some of them support other sizes as well. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks.

Fifteen proposals meeting NIST's basic criteria were submitted in 1998 and subjected to intense discussion and analysis, "round one" evaluation. In August 1999, NIST narrowed the field to five "round two" candidates:

- Mars from IBM
- RC6 from RSA
- Rijndael from two Belgian researchers
- Serpent, a British-Norwegian-Israeli research collaboration
- Twofish from the consulting firm Counterpane

We expect IPSEC will eventually use the AES winner, and we expect to see a winner (or more than one; there is an ongoing discussion on that point) declared in the summer of 2000.

Adding one or more AES ciphers to Linux FreeS/WAN would be useful undertaking, and considerable freely available code exists to start from. One complication is that our code is built for a 64-bit block cipher and AES uses a 128-bit block. Volunteers via the mailing list would be welcome.

For more information, see the NIST AES home page or the Block Cipher Lounge AES page. For code and benchmarks see Brian Gladman's page .

AH
: The IPSEC Authentication Header, added after the IP header. For details, see our IPSEC Overview document and/or RFC 2402.

Alice and Bob
: A and B, the standard example users in writing on cryptography and coding theory. Carol and Dave join them for protocols which require more players.

Bruce Schneier extends these with many others such as Eve the Eavesdropper and Victor the Verifier. His extensions seem to be in the process of becoming standard as well. See page 23 of Applied Cryptography

Alice and Bob have an amusing biography on the web.

ARPA
: see DARPA

ASIO
: Australian Security Intelligence Organisation.

Asymmetric cryptography
: See public key cryptography.

Authentication
: Ensuring that a message originated from the expected sender and has not been altered on route. IPSEC uses authentication in two places:

- authenticating the players in IKE's Diffie-Hellman key exchanges to prevent man-in-the-middle attacks. This can be done in a number of ways. The methods supported by FreeS/WAN are discussed in our configuration document.
- authenticating packets on an established SA, either with a separate authentication header or with the optional authentication in the ESP protocol. In either case, packet authentication uses a hashed message athentication code technique.

Outside IPSEC, passwords are perhaps the most common authentication mechanism. Their function is essentially to authenticate the person's identity to the system. Passwords are generally only as secure as the network they travel over. If you send a cleartext password over a tapped phone line or over a network with a packet sniffer on it, the security provided by that password becomes zero. Sending an encrypted password is no better; the attacker merely records it and reuses it at his convenience. This is called a replay attack.

A common solution to this problem is a challenge-response system. This defeats simple eavesdropping and replay attacks. Of course an attacker might still try to break the cryptographic algorithm used, or the random number generator.

Automatic keying
: A mode in which keys are automatically generated at connection establisment and new keys automaically created periodically thereafter. Contrast with manual keying in which a single stored key is used.

IPSEC uses the Diffie-Hellman key exchange protocol to create keys. An authentication mechansim is required for this. The methods supported by FreeS/WAN are discussed in our configuration document.

Having an attacker break the authentication is emphatically not a good idea. An attacker that breaks authentication, and manages to subvert some other network entities (DNS, routers or gateways), can use a man-in-the middle attack to break the security of your IPSEC connections.

However, having an attacker break the authentication in automatic keying is not quite as bad as losing the key in manual keying.

- An attacker who reads /etc/ipsec.conf and gets the keys for a manually keyed connection can, without further effort, read all messages encrypted with those keys, including any old messages he may have archived.
- Automatic keying has a property called perfect forward secrecy. An attacker who breaks the authentication gets none of the automatically generated keys and cannot immediately read any messages. He has to mount a successful man-in-the-middle attack in real time before he can read anything. He cannot read old archived messages at all and will not be able to read any future messages not caught by man-in-the-middle tricks.

That said, the secrets used for authentication, stored in ipsec.secrets(5), should still be protected as tightly as cryptographic keys.

Bay Networks

A vendor of routers, hubs and related products, now a subsidiary of Northern Telecom. Interoperation between their IPSEC products and Linux FreeS/WAN was problematic at last report; see our compatibility document.

benchmarks

Our default block cipher, triple DES, is slower than many alternate ciphers that might be used. Speeds achieved, however, seem adequate for many purposes. For example, the assembler code from the LIBDES library we use encrypts 1.6 megabytes per second on a Pentium 200, according to the test program supplied with the library.

The University of Wales at Aberystwyth has done quite detailed tests and put their results on the web.

Even a 486 can handle a T1 line, according to this mailing list message:

```
Subject: Re: linux-ipsec: IPSec Masquerade
   Date: Fri, 15 Jan 1999 11:13:22 -0500
   From: Michael Richardson

. . . A 486/66 has been clocked by Phil Karn to do
10Mb/s encryption.. that uses all the CPU, so half that to get some CPU,
and you have 5Mb/s. 1/3 that for 3DES and you get 1.6Mb/s....
```

From an Internet Draft *The ESP Triple DES Transform:*

```
    Phil Karn has tuned DES-EDE3-CBC software to achieve 6.22 Mbps with a
    133 MHz Pentium.  Other DES speed estimates may be found at
    [Schneier95, page 279].  Your milage may vary.
```

If you want to measure the loads FreeS/WAN puts on a system, note that tools such as top or measurements such as load average are more-or-less useless for this. They are not designed to measure something that does most of its work inside the kernel.

BIND

Berkeley Internet Name Daemon, a widely used implementation of DNS (Domain Name Service). See our bibliography for a useful reference. See the BIND home page for more information and the latest version.

Birthday attack

A cryptographic attack based on the mathematics exemplified by the birthday paradox. This math turns up whenever the question of two cryptographic operations producing the same result becomes an issue:

- collisions in message digest functions.
- identical output blocks from a block cipher
- repetition of a challenge in a challenge-response system

Resisting such attacks is part of the motivation for:

- hash algorithms such as SHA and RIPEMD-160 giving a 160-bit result rather than the 128 bits of MD4, MD5 and RIPEMD-128.
- AES block ciphers using a 128-bit block instead of the 64-bit block of most current ciphers
- IPSEC using a 32-bit counter for packets sent on an automatically keyed SA and requiring that the connection always be rekeyed before the counter overflows.

Birthday paradox

Not really a paradox, just a rather counter-intuitive mathematical fact. In a group of 23 people, the chance of a least one pair having the same birthday is over 50%.

The second person has 1 chance in 365 (ignoring leap years) of matching the first. If they don't match, the third person's chances of matching one of them are 2/365. The 4th, 3/365, and so on. The total of these chances grows more quickly than one might guess.

Block cipher

A symmetric cipher which operates on fixed-size blocks of plaintext, giving a block of ciphertext for each. Contrast with stream cipher. Block ciphers can be used in various modes when multiple block are to be encrypted.

DES is among the the best known and widely used block ciphers, but is now obsolete. Its 56-bit key size makes it highly insecure today. Triple DES is the default transform for Linux FreeS/WAN because it is the only cipher which is both required in the RFCs and apparently secure.

The current generation of block ciphers -- such as Blowfish, CAST-128 and IDEA -- all use 64-bit blocks and 128-bit keys. The next generation, AES, uses 128-bit blocks and supports key sizes up to 256 bits.

The Block Cipher Lounge web site has more information.

Blowfish

A block cipher using 64-bit blocks and keys of up to 448 bits, designed by Bruce Schneier and used in several products.

This is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN.

Brute force attack (exhaustive search)

Breaking a cipher by trying all possible keys. This is always possible in theory (except against a one-time pad), but it becomes practical only if the key size is inadequate. For an important example, see our document on the insecurity of DES with its 56-bit key. For an analysis of key sizes required to resist plausible brute force attacks, see this paper.

Longer keys protect against brute force attacks. Each extra bit in the key doubles the number of possible keys and therefore doubles the work a brute force attack must do. A large enough key defeats **any** brute force attack.

For example, the EFF's DES Cracker searches a 56-bit key space in an average of a few days. Let us assume an attacker that can find a 64-bit key (256 times harder) by brute force search in a second (a few hundred thousand times faster). For a 96-bit key, that attacker needs 2^{32} seconds, just over a century. Against a 128-bit key, he needs 2^{32} centuries or about 400,000,000,000 years. Your data is then obviously secure against brute force attacks. Even if our estimate of the attacker's speed is off by a factor of a million, it still takes him 400,000 years to crack a message.

This is why

- single DES is now considered dangerously insecure
- any cipher we add to Linux FreeS/WAN will have *at least* a 90-bit key
- all of the current generation of block ciphers use a 128-bit or longer key
- AES ciphers support keysizes 128, 192 and 256 bits

Cautions:
Inadequate keylength always indicates a weak cipher but it is important to note that *adequate keylength does not necessarily indicate a strong cipher*. There are many attacks other than brute force, and adequate keylength *only* guarantees resistance to brute force. Any cipher, whatever its key size, will be weak if design or implementation flaws allow other attacks.

Also, *once you have adequate keylength* (somewhere around 90 or 100 bits), *adding more key bits make no practical difference*, even against brute force. Consider our 128-bit example above that takes 400 billion years to break by brute force. Do we care if an extra 16 bits of key put that into the quadrillions? No. What about 16 fewer bits reducing it to the 112-bit security level of Triple DES, which our example attacker could break in just over a billion years? No again, unless we're being really paranoid about safety margins.

There may be reasons of convenience in the design of the cipher to support larger keys. For example Blowfish allows up to 448 bits and RC4 up to 2048, but beyond 100-odd bits it makes no difference to practical security.

Bureau of Export Administration
: see BXA

BXA
: The US Commerce Department's **B**ureau of Export Administration which administers the EAR Export Administration Regulations controling the export of, among other things, cryptography.

CA
: Certification Authority, an entity in a public key infrastructure that can certify keys by signing them. Usually CAs form a hierarchy. The top of this hierarchy is called the root CA.

See Web of Trust for an alternate model.

CAST-128
: A block cipher using 64-bit blocks and 128-bit keys, described in RFC 2144 and used in products such as Entrust and recent versions of PGP.

This is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN.

CAST-256
: Entrust's candidate cipher for the AES standard, largely based on the CAST-128 design.

CBC mode
: Cipher Block Chaining mode, a method of using a block cipher in which for each block except the first, the result of the previous encryption is XORed into the new block before it is encrypted. CBC is the mode used in IPSEC.

  An initialisation vector (IV) must be provided. It is XORed into the first block before encryption. The IV need not be secret but should be different for each message and unpredictable.

Certification Authority
: see CA

Cipher Modes
: Different ways of using a block cipher when encrypting multiple blocks.

  Four standard modes were defined for DES in FIPS 81. They can actually be applied with any block cipher.

ECB	Electronic CodeBook	encrypt each block independently
CBC	Cipher Block Chaining	XOR previous block ciphertext into new block plaintext before encrypting new block
CFB	Cipher FeedBack	
OFB	Output FeedBack	

  IPSEC uses CBC mode since this is only marginally slower than ECB and is more secure. In ECB mode the same plaintext always encrypts to the same ciphertext, unless the key is changed. In CBC mode, this does not occur.

  Various other modes are also possible, but none of them are used in IPSEC.

Challenge-response authentication
: An authentication system in which one player generates a random number, encrypts it and sends the result as a challenge. The other player decrypts and sends back the result. If the result is correct, that proves to the first player that the second player knew the appropriate secret, required for the decryption.

  Variations on this technique exist using public key or symmetric cryptography. Some provide two-way authentication, assuring each player of the other's identity.

  Because the random number is different each time, this defeats simple eavesdropping and replay attacks. Of course an attacker might still try to break the cryptographic algorithm used, or the random number generator.

Ciphertext
: The encrypted output of a cipher, as opposed to the unencrypted plaintext input.

Cisco
: A vendor of routers, hubs and related products. Their IPSEC products interoperate with Linux FreeS/WAN; see our compatibility document.

Conventional cryptography
: See symmetric cryptography

Collision resistance
: The property of a message digest algorithm which makes it hard for an attacker to find or construct two inputs which hash to the same output.

Copyleft
: see GNU General Public License

CSE
: Communications Security Establishment, the Canadian organisation for signals intelligence.

DARPA (sometimes just ARPA)
: The US government's **D**efense **A**dvanced **R**esearch **P**rojects **A**gency. Projects they have funded over the years have included the Arpanet which evolved into the Internet, the TCP/IP protocol suite (as a replacement for the original Arpanet suite), the Berkeley 4.x BSD Unix projects, and Secure DNS.

  For current information, see their web site.

Denial of service (DOS) attack
: An attack that aims at denying some service to legitimate users of a system, rather than providing a service to the attacker.

  - One variant is a flooding attack, overwhelming the system with too many packets, to much email, or whatever.
  - A closely related variant is a resource exhaustion attack. For example, consider a "TCP SYN flood" attack. Setting up a TCP connection involves a three-packet exchange:
    - Initiator: Connection please (SYN)
    - Responder: OK (ACK)
    - Initiator: OK here too

    If the attacker puts bogus source information in the first packet, such that the second is never delivered, the responder may wait a long time for the third to come back. If responder has already allocated memory for the connection data structures, and if many of these bogus packets arrive, the responder may run out of memory.
  - Another variant is to feed the system undigestible data, hoping to make it sick. For example, IP packets are limited in size to 64K bytes and a fragment carries information on where it starts within that 64K and how long it is. The "ping of death" delivers fragments that say, for example, that they start at 60K and are 20K long. Attempting to re-assemble thse without checking for overflow can be fatal.

  The two example attacks discussed were both quite effective when first discovered, capable of crashing or disabling many operating systems. They were also well-publicised, and today far fewer systems are vulnerable to them.

DES
: The **D**ata **E**ncryption **S**tandard, a block cipher with 64-bit blocks and a 56-bit key. Probably the most widely used symmetric cipher ever devised. DES has been a US government standard for their own use (only for unclassified data), and for some regulated industries such as banking, since the late 70's.

  DES is seriously insecure against current attacks.

  Linux FreeS/WAN includes DES since the RFCs require it, but our default configuration refuses to negotiate a connection using it. **We strongly recommend that single DES not be used.**

  See also 3DES and DESX, stronger ciphers based on DES.

DESX
: An improved DES suggested by Ron Rivest of RSA Data Security. It XORs extra key material into the text before and after applying the DES cipher.

  This is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN. DESX would be the easiest additional transform to add; there would be very little code to write. It would be much faster than 3DES and almost certainly more secure than DES. However, since it is not in the RFCs other IPSEC implementations cannot be expected to have it.

DH
: see Diffie-Hellman

Diffie-Hellman (DH) key exchange protocol
: A protocol that allows two parties without any initial shared secret to create one in a manner immune to eavesdropping. Once they have done this, they can communicate privately by using that shared secret as a key for a block cipher or as the basis for key exchange.

  The protocol is secure against all passive attacks, but it is not at all resistant to active man-in-the-middle attacks. If a third party can impersonate Bob to Alice and vice versa, then no useful secret can be created. Authentication is a prerequisite for safe Diffie-Hellman key exchange.

  IPSEC can use any of several authentication mechanisims. Those supported by FreeS/WAN are discussed in our configuration document.

Digital signature
: Take a message digest of a document and encrypt it with your private key for some public key cryptosystem. I can decrypt with your public key and verify that the result matches the digest I calculate. This proves that the encrypted digest was created with your private key.

  Such an encrypted message digest can be treated as a signature since it cannot be created without *both* the document *and* the private key which only you should possess. The legal issues are complex, but several countries are moving in the direction of legal recognition for digital signatures.

DNS
: **D**omain **N**ame **S**ervice, a distributed database through which names are associated with numeric addresses and other information in the Internet Protocol Suite. See also BIND, the Berkeley Internet Name Daemon which implements DNS services and Secure DNS. See our bibliography for a useful reference on both.

DOS attack
: see Denial Of Service attack

EAR
: The US government's **E**xport **A**dministration **R**egulations, administered by the Bureau of Export Administration. These have replaced the earlier ITAR regulations as the controls on export of cryptography.

ECB mode
: **E**lectronic **C**ode**B**ook mode, the simplest way to use a block cipher. See Cipher Modes.

EDE
: The sequence of operations normally used in either the three-key variant of triple DES used in IPSEC or the two-key variant used in some other systems.

The sequence is:

- Encrypt with key1
- Decrypt with key2
- Encrypt with key3

For the two-key version, key1=key3.

The "advantage" of this EDE order of operations is that it makes it simple to interoperate with older devices offering only single DES. Set key1=key2=key3 and you have the worst of both worlds, the overhead of triple DES with the security of single DES. Since single DES is insecure, this is a rather dubious "advantage".

The EDE two-key variant can also interoperate with the EDE three-key variant used in IPSEC; just set k1=k3.

Entrust
: A Canadian company offerring enterprise PKI products using CAST-128 symmetric crypto, RSA public key and X.509 directories.

EFF
: Electronic Frontier Foundation, an advocacy group for civil rights in cyberspace.

Encryption
: Techniques for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. A key is required to read the message.

Major variants include symmetric encryption in which sender and receiver use the same secret key and public key methods in which the sender uses one of a matched pair of keys and the receiver uses the other. Many current systems, including IPSEC, are hybrids combining the two techniques.

ESP
: Encapsulated Security Payload, the IPSEC protocol which provides encryption. It can also provide authentication service and may be used with null encryption (which we do not recommend). For details see our IPSEC Overview document and/or RFC 2406.

Extruded subnet
: A situation in which something IP sees as one network is actually in two or more places.

For example, the Internet may route all traffic for a particular company to that firm's corporate gateway. It then becomes the company's problem to get packets to various machines on their subnets in various departments. They may decide to treat a branch office like a subnet, giving it IP addresses "on" their corporate net. This becomes an extruded subnet.

Packets bound for it are delivered to the corporate gateway, since as far as the outside world is concerned, that subnet is part of the corporate network. However, instead of going onto the corporate LAN (as they would for, say, the accounting department) they are then encapsulated and sent back onto the Internet for delivery to the branch office.

For information on doing this with Linux FreeS/WAN, look in our Configuration file.

Exhaustive search
: See brute force attack.

FIPS

Federal Information Processing Standard, the US government's standards for products it buys. These are issued by NIST. Among other things, DES and SHA are defined in FIPS documents. NIST have a FIPS home page.

Free Software Foundation (FSF)

An organisation to promote free software, free in the sense of these quotes from their web pages

> "Free software" is a matter of liberty, not price. To understand the concept, you should think of "free speech", not "free beer."
>
> "Free software" refers to the users' freedom to run, copy, distribute, study, change and improve the software.

See also GNU, GNU General Public License, and the FSF site.

FreeSWAN

see Linux FreeS/WAN

FSF

see Free software Foundation

GCHQ

Government Communications Headquarters, the British organisation for signals intelligence.

GILC

Global Internet Liberty Campaign, an international organisation advocating, among other things, free availability of b cryptography. They have a campaign to remove cryptographic software from the Wassenaar Arrangement.

Global Internet Liberty Campaign

see GILC.

Global Trust Register

An attempt to create something like a root CA for PGP by publishing both as a book and on the web the fingerprints of a set of verified keys for well-known users and organisations.

GMP

The GNU Multi-Precision library code, used in Linux FreeS/WAN by Pluto for public key calculations.

GNU

GNU's Not Unix, the Free Software Foundation's project aimed at creating a free system with at least the capabilities of Unix. Linux uses GNU utilities extensively.

GPG

see GNU Privacy Guard

GNU General Public License (GPL, copyleft)

The license developed by the Free Software Foundation under which Linux, Linux FreeS/WAN and many other pieces of software are distributed. The license allows anyone to redistribute and modify the code, but forbids anyone from distributing executables without providing access to source code. For more details see the file COPYING included with GPLed source distributions, including ours, or the GNU site's GPL page.

GNU Privacy Guard

An open source implementation of Open PGP as defined in RFC 2440.

GPL

see GNU General Public License.

Hash

see message digest

Hashed Message Authentication Code (HMAC)

using keyed message digest functions to authenticate a message. This differs from other uses of these functions:

- In normal usage, the hash function's internal variable are initialised in some standard way. Anyone can reproduce the hash to check that the message has not been altered.
- For HMAC usage, you initialise the internal variables from the key. Only someone with the key can reproduce the hash. A successful check of the hash indicates not only that the message is unchanged but also that the creator knew the key.

The exact techniques used in IPSEC are defined in RFC 2104. They are referred to as HMAC-MD5-96 and HMAC-SHA-96 because they output only 96 bits of the hash. This makes some attacks on the hash functions harder.

HMAC
: see Hashed Message Authentication Code

HMAC-MD5-96
: see Hashed Message Authentication Code

HMAC-SHA-96
: see Hashed Message Authentication Code

Hybrid cryptosystem
: A system using both public key and symmetric cipher techniques. This works well. Public key methods provide key management and digital signature facilities which are not readily available using symmetric ciphers. The symmetric cipher, however, can do the bulk of the encryption work much more efficiently than public key methods.

IAB
: Internet Architecture Board.

ICMP
: **I**nternet **C**ontrol **M**essage **P**rotocol. This is used for various IP-connected devices to manage the network.

IDEA
: **I**nternational **D**ata **E**ncrypion **A**lgorithm, developed in Europe as an alternative to exportable American ciphers such as DES which were too weak for serious use. IDEA is a block cipher using 64-bit blocks and 128-bit keys, and is used in products such as PGP.

IDEA is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN.

IDEA is patented and, with strictly limited exceptions for personal use, using it requires a license from Ascom.

IESG
: Internet Engineering Steering Group.

IETF
: Internet Engineering Task Force, the umbrella organisation whose various working groups make most of the technical decisions for the Internet. The IETF IPSEC working group wrote the RFCs we are implementing.

IKE
: **I**nternet **K**ey **E**xchange, based on the Diffie-Hellman key exchange protocol. IKE is implemented in Linux FreeS/WAN by the Pluto daemon.

Initialisation Vector (IV)
: Some cipher modes, including the CBC mode which IPSEC uses, require some extra data at the beginning. This data is called the initialisation vector. It need not be secret, but should be different for each message. Its function is to prevent messages which begin with the same text from encrypting to the same ciphertext. That might give an analyst an opening, so it is best prevented.

IP
: **I**nternet **P**rotocol.

IP masquerade

A method of allowing multiple machines to communicate over the Internet when only one IP address is available for their use. See the Linux masquerade resource page for details.

The client machines are set up with reserved non-routable IP addresses defined in RFC 1918. The masquerading gateway, the machine with the actual link to the Internet, rewrites packet headers so that all packets going onto the Internet appear to come from one IP address, that of its Internet interface. It then gets all the replies, does some table lookups and more header rewriting, and delivers the replies to the appropriate client machines.

To use masquerade with Linux FreeS/WAN, you must set leftfirewall=yes and/or rightfirewall=yes in the connection description in /etc/ipsec.conf.

IPng
: "IP the Next Generation", see IPv6.

IPv4
: The current version of the Internet protocol suite.

IPv6 (IPng)
: Version six of the Internet protocol suite, currently being developed. It will replace the current version four. IPv6 has IPSEC as a mandatory component.

  See this web site for more details.

IPSEC
: **I**nternet **P**rotocol **SEC**urity, security functions (authentication and encryption) implemented at the IP level of the protocol stack. It is optional for IPv4 and mandatory for IPv6.

  This is the standard Linux FreeS/WAN is implementing. For more details, see our IPSEC Overview. For the standards, see RFCs listed in our RFCs document.

ISAKMP
: **I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol, defined in RFC 2408.

ITAR
: **I**nternational **T**raffic in **A**rms **R**egulations, US regulations administered by the State Department which until recently limited export of, among other things, cryptographic technology and software. ITAR still exists, but the limits on cryptography have now been transferred to the Export Administration Regulations under the Commerce Department's Bureau of Export Administration.

IV
: see Initialisation vector

Keyed message digest
: See HMAC.

Key length
: see brute force attack

KLIPS
: **K**erne**l** **IP** **S**ecurity, the Linux FreeS/WAN project's changes to the Linux kernel to support the IPSEC protocols.

LDAP
: **L**ightweight **D**irectory **A**ccess **P**rotocol, defined in RFCs 1777 and 1778, a method of accessing information stored in directories. LDAP is used by several PKI implementations, often with X.501 directories and X.509 certificates. It may also be used by IPSEC to obtain key certifications from those PKIs. This is not yet implemented in Linux FreeS/WAN.

LIBDES

A publicly available library of DES code, written by Eric Young, which Linux FreeS/WAN uses in both KLIPS and Pluto.

Linux

A freely available Unix-like operating system based on a kernel originally written for the Intel 386 architecture by (then) student Linus Torvalds. Once his 32-bit kernel was available, the GNU utilities made it a usable system and contributions from many others led to explosive growth.

Today Linux is a complete Unix replacement available for several CPU architectures -- Intel, DEC/Compaq Alpha, Power PC, both 32-bit SPARC and the 64-bit UltraSPARC, SrongARM, . . . -- with support for multiple CPUs on some architectures.

Linux FreeS/WAN is intended to run on all CPUs supported by Linux and is currently (February 1999) known to work on Intel, Alpha and StrongARM. See our compatibility document for details.

Linux FreeS/WAN

Our implementation of the IPSEC protocols, intended to be freely redistributable source code with a GNU GPL license and no constraints under US or other export laws. Linux FreeS/WAN is intended to interoperate with other IPSEC implementations. The name is partly taken, with permission, from the S/WAN multi-vendor IPSEC compatability effort. Linux FreeS/WAN has two major components, KLIPS (KerneL IPSEC Support) and the Pluto daemon which manages the whole thing.

See our IPSEC Overview for more detail. For the code see our primary distribution site or one of the mirror sites on this list.

Mailing list

The Linux FreeS/WAN project has an open public email list for bug reports and software development discussions. The list address is **linux-ipsec@clinet.fi**. To subscribe, send mail to majordomo@clinet.fi with a one-line message body "subscribe linux-ipsec". For more information, send majordomo the one-line message "help".

NOTE: **US citizens or residents are asked not to post code to the list, not even one-line bug fixes.** The project cannot accept code which might entangle it in US export restrictions.

For more detail, see our document on this and other mailing lists.

Man-in-the-middle attack

An active attack in which the attacker impersonates each of the legitimate players in a protocol to the other.

For example, if Alice and Bob are negotiating a key via the Diffie-Hellman key agreement, and are not using authentication to be certain they are talking to each other, then an attacker able to insert himself in the communication path can deceive both players.

Call the attacker Mallory. For Bob, he pretends to be Alice. For Alice, he pretends to be Bob. Two keys are then negotiated, Alice-to-Mallory and Bob-to-Mallory. Alice and Bob each think the key they have is Alice-to-Bob.

A message from Alice to Bob then goes to Mallory who decrypts it, reads it and/or saves a copy, re-encrypts using the Bob-to-Mallory key and sends it along to Bob. Bob decrypts successfully and sends a reply which Mallory decrypts, reads, re-encrypts and forwards to Alice.

To make this attack effective, Mallory must

- subvert some part of the network in some way that lets him carry out the deception
  possible targets: DNS, router, Alice or Bob's machine, mail server, ...
- beat any authentication mechanism Alice and Bob use
  strong authentication defeats the attack entirely; this is why IKE requires authentication
- work in real time, delivering messages without noticable delay
  not hard if Alice and Bob are using email; quite difficult in some situations.

If he manages it, however, it is devastating. He not only gets to read all the messages; he can alter messages, inject his own, forge anything he likes, . . . In fact, he controls the communication completely.

Manual keying
: An IPSEC mode in which the keys are provided by the administrator. In FreeS/WAN, they are stored in /etc/ipsec.conf. The alternative, automatic keying, is preferred in most cases.

MD4
: Message Digest Algorithm Four from Ron Rivest of RSA. MD4 was widely used a few years ago, but is now considered obsolete. It has been replaced by its descendants MD5 and SHA.

MD5
: Message Digest Algorithm Five from Ron Rivest of RSA, an improved variant of his MD4. Like MD4, it produces a 128-bit hash. For details see RFC 1321.

MD5 is one of two message digest algorithms available in IPSEC. The other is SHA. SHA produces a longer hash and is therefore more resistant to birthday attacks, but this is not a concern for IPSEC. The HMAC method used in IPSEC is secure even if the underlying hash is not particularly strong against this attack.

Meet-in-the-middle attack
: A divide-and-conquer attack which breaks a cipher into two parts, works against each separately, and compares results. Probably the best known example is an attack on double DES. This applies in principle to any pair of block ciphers, e.g. to an encryption system using, say, CAST-128 and Blowfish, but we will describe it for double DES.

Double DES encryption and decryption can be written:

```
C = E(k2,E(k1,P))
P = D(k1,D(k2,C))
```

Where C is ciphertext, P is plaintext, E is encryption, D is decryption, k1 is one key, and k2 is the other key. If we know a P, C pair, we can try and find the keys with a brute force attack, trying all possible k1, k2 pairs. Since each key is 56 bits, there are 2^{112} such pairs and this attack is painfully inefficient.

The meet-in-the middle attack re-writes the equations to calculate a middle value M:

```
M = E(k1,P)
M = D(k2,C)
```

Now we can try some large number of D(k2,C) decryptions with various values of k2 and store the results in a table. Then start doing E(k1,P) encryptions, checking each result to see if it is in the table.

With enough table space, this breaks double DES with 2^{57} work. The memory requirements of such attacks can be prohibitive, but there is a whole body of research literature on methods of reducing them.

Message Digest Algorithm
: An algorithm which takes a message as input and produces a hash or digest of it, a fixed-length set of bits which depend on the message contents in some highly complex manner. Design criteria include making it extremely difficult for anyone to counterfeit a digest or to change a message without altering its digest. One essential property is collision resistance. The main applications are in message authentication and digital signature schemes. Widely used algorithms include MD5 and SHA. In IPSEC, message digests are used for HMAC authentication of packets.

MTU
: Maximum Transmission Unit, the largest size of packet that can be sent over a link. This is determined by the underlying network, but must be taken account of at the IP level.

IP packets, which can be up to 64K bytes each, must be packaged into lower-level packets of the appropriate size for the underlying network(s) and re-assembled on the other end. When a packet must pass over multiple networks, each with its own MTU, and many of the MTUs are unknown to the sender, this becomes a fairly complex problem. See path MTU discovery for details.

Often the MTU is a few hundred bytes on serial links and 1500-odd on Ethernet. There are, however, serial link protocols which use a larger MTU to avoid packet packet fragmentation at the ethernet/serial boundary, and newer (especially gigabit) Ethernet networks sometimes support much larger packets because these are more efficient in some applications.

NAI
: Network Associates, a conglomerate formed from PGP Inc., TIS, Macaffee Anti-virus products and several others. Among other things, they offer an IPSEC-based VPN.

NAT
: Network Address Translation.

NIST
: The US National Institute of Standards and Technology, responsible for FIPS standards including DES and its replacement, AES.

Nonce
: A random value used in an authentication protocol.

Non-routable IP address
: An IP address not normally allowed in the "to" or "from" IP address field header of IP packets.

Almost invariably, the phrase "non-routable address" means one of the addresses reserved by RFC 1918 for private networks:

- 10.anything
- 172.x.anything with 16 <= x <= 31
- 192.168.anything

These addresses are commonly used on private networks, e.g. behind a Linux machines doing IP masquerade. Machines within the private network can address each other with these addresses. All packets going outside that network, however, have these addresses replaced before they reach the Internet.

If any packets using these addresses do leak out, they do not go far. Most routers automatically discard all such packets.

Various other addresses -- the 127.0.0.0/8 block reserved for local use, 0.0.0.0, various broadcast and network addresses -- cannot be routed over the Internet, but are not normally included in the meaning when the phrase "non-routable address" is used.

NSA

The US National Security Agency, the American organisation for signals intelligence, the protection of US government messages and the interception and analysis of other messages. For details, see Bamford's "The Puzzle Palace".

Some history of NSA documents were declassified in response to a FOIA (Freedom of Information Act) request.

Oakley

A key determination protocol, defined in RFC 2412.

One time pad

A cipher in which the key is:

- as long as the total set of messages to be enciphered
- absolutely random
- never re-used

Given those three conditions, it can easily be proved that the cipher is perfectly secure, in the sense that an attacker with intercepted message in hand has no better chance of guessing the message than an attacker who only knows the message length. No such proof exists for any other cipher.

There are, however, several problems with this "perfect" cipher.

- It is wildly impractical for many applications. Key management is difficult or impossible.
- It is *extremely* fragile. Small changes which violate the conditions listed above do not just weaken the cipher a bit; quite often they destroy its security completely.
  - Re-using the pad weakens it to the point where it can be broken with pencil and paper. With a computer, the attack is trivially easy.
  - Using computer-generated pseudo-random numbers instead of a really random pad completely invalidates the security proof. Depending on random number generator used, this may also give an extremely weak cipher.
- If an attacker knows the plaintext and has an intercepted message, he can discover the pad. This does not matter if the attacker is just a passive eavesdropper. It gives him no plaintext he didn't already know and we don't care that he learns a pad which we'll never re-use. However, knowing the pad lets an active attacker perform a man-in-the-middle attack, replacing your message with whatever he chooses.

Outrageous marketing claims about the "unbreakable" security of various products which somewhat resemble one-time pads are common. They are a sure sign of cryptographic snake oil.

See also the one time pad FAQ.

Opportunistic encryption

A situation in which any two IPSEC-aware machines can secure their communications, without a pre-shared secret and without a common PKI. This is a long-term goal of the Linux FreeS/WAN project which we expect to acheive using Secure DNS.

P1363 standard
: An IEEE standard for public key cryptography.

Passive attack
: An attack in which the attacker only eavesdrops and attempts to analyse intercepted messages, as opposed to an active attack in which he diverts messages or generates his own.

Path MTU discovery
: The process of discovering the largest packet size which all links on a path can handle without fragmentation -- that is, without any router having to break the packet up into smaller pieces to match the MTU of its outgoing link.

This is done as follows:

- originator sends the largest packets allowed by MTU of the first link, setting the DF (don't fragment) bit in the packet header
- any router which cannot send the packet on (outgoing MTU is too small for it, and DF prevents fragmenting it to match) sends back an ICMP packet reporting the problem
- originator looks at ICMP message and tries a smaller size
- eventually, you settle on a size that can pass all routers
- thereafter, originator just sends that size and no-one has to fragment

Since this requires co-operation of many systems, and since the next packet may travel a different path, this is one of the trickier areas of IP programming. Bugs that have shown up over the years have included:

- malformed ICMP messages
- hosts that ignore or mishandle these ICMP messages
- firewalls blocking the ICMP messages so host does not see them

Since IPSEC adds a header, it increases packet size and may require fragmentation even where incoming and outgoing MTU are equal.

Perfect forward secrecy (PFS)
: A property of systems such as Diffie-Hellman key exchange which use a long-term key (the shared secret in IKE) and generate short-term keys as required. If an attacker who acquires the long-term key *provably* can

- *neither* read previous messages which he may have archived
- *nor* read future messages without performing additional successful attacks

then the system has PFS. The attacker needs the short-term keys in order to read the traffic and merely having the long-term key does not allow him to infer those. Of course, it may allow him to conduct another attack (such as man-in-the-middle) which gives him some short-term keys, but he does not automatically get them just by acquiring the long-term key.

PFS
: see Perfect Forward Secrecy

PGP
: Pretty Good Privacy, a personal encryption system for email based on public key technology, written by Phil Zimmerman.

The 2.xx versions of PGP used the RSA public key algorithm and used IDEA as the symmetric cipher. These versions are described in RFC 1991 and in Garfinkel's book. They are freely available. There is a US version and an International version . The differences are questions of licensing; the two are fully compatible.

Since version 5, the products from PGP Inc. have used Diffie-Hellman public key methods and IDEA or CAST-128 symmetric encryption. These can verify signatures from the 2.xx versions, but cannot exchange encryted messages with them. Some 5.x and 6.x products are free for personal use. Information on all products and downloads of the free ones are available from PGP Inc. The free versions are also on the US and International sites listed above.

An IETF working group has issued RFC 2440 for an "Open PGP" standard, similar to the 5.x versions. PGP Inc. staff were among the authors. A free Gnu Privacy Guard based on that standard is now available.

PGP Inc.
: A company founded by Zimmerman, the author of PGP, now a division of NAI. See the corporate website.

  Their PGP 6.5 product includes PGPnet, an IPSEC client for Macintosh or for Windows 95/98/NT.

Photuris
: Another key negotiation protocol, an alternative to IKE, described in RFCs 2522 and 2523.

PPTP
: **P**oint-to-**P**oint **T**unneling **P**rotocol.

PKI
: **P**ublic **K**ey **I**nfrastructure, the things an organisation or community needs to set up in order to make public key cryptographic technology a standard part of their operating procedures.

  There are several PKI products on the market. Typically they use a hierarchy of Certification Authorities (CAs). Often they use LDAP access to X.509 directories to implement this.

  See Web of Trust for a different sort of infrastructure.

PKIX
: **PKI** e**X**change, an IETF standard that allows PKIs to talk to each other.

  This is required, for example, when users of a corporate PKI need to communicate with people at client, supplier or government organisations, any of which may have a different PKI in place. I should be able to talk to you securely whenever:

  - your organisation and mine each have a PKI in place
  - you and I are each set up to use those PKIs
  - the two PKIs speak PKIX
  - the configuration allows the conversation

  At time of writing (March 1999), this is not yet widely implemented but is under quite active development by several groups.

Plaintext
: The unencrypted input to a cipher, as opposed to the encrypted ciphertext output.

Pluto
: The Linux FreeS/WAN daemon which handles key exchange via the IKE protocol, connection negotiation, and other higher-level tasks. Pluto calls the KLIPS kernel code as required. For details, see the manual page ipsec_pluto(8).

Public Key Cryptography
: In public key cryptography, keys are created in matched pairs. Encrypt with one half of a pair and only the matching other half can decrypt it. This contrasts with symmetric or secret key cryptography in which a single key known to both parties is used for both encryption and decryption.

One half of each pair, called the public key, is made public. The other half, called the private key, is kept secret. Messages can then be sent by anyone who knows the public key to the holder of the private key. Encrypt with the public key and you know only someone with the matching private key can decrypt.

Public key techniques can be used to create digital signatures and to deal with key management issues, perhaps the hardest part of effective deployment of symmetric ciphers. The resulting hybrid cryptosystems use public key methods to manage keys for symmetric ciphers.

Many organisations are currently creating PKIs, public key infrastructures to make these benefits widely available.

Public Key Infrastructure
: see PKI

Random
: A remarkably tricky term, far too much so for me to attempt a definition here. Quite a few cryptosystems have been broken via attacks on weak random number generators, even when the rest of the system was sound.

See RFC 1750 for the theory. It will be available locally if you have downloaded our RFC bundle (which is described here). Or read it on the net.

See the manual pages for ipsec_ranbits(8) and random(4) for details of what we use.

There has recently been discussion on several mailing lists of the limitations of Linux /dev/random and of whether we are using it correctly. Those discussions are archived on the /dev/random support page.

Raptor
: A firewall product for Windows NT offering IPSEC-based VPN services. Linux FreeS/WAN interoperates with Raptor; see our Compatibility document for details. Raptor have recently merged with Axent.

RC4
: Rivest Cipher four, designed by Ron Rivest of RSA and widely used. Believed highly secure with adequate key length, but often implemented with inadequate key length to comply with export restrictions.

RC6
: Rivest Cipher six, RSA's AES candidate cipher.

Replay attack
: An attack in which the attacker records data and later replays it in an attempt to deceive the recipient.

RFC
: Request For Comments, an Internet document. Some RFCs are just informative. Others are standards.

Our list of IPSEC and other security-related RFCs is here, along with information on methods of obtaining them.

RIPEMD
: A message digest algorithm. The current version is RIPEMD-160 which gives a 160-bit hash.

Root CA
: The top level Certification Authority in a hierachy of such authorities.

Routable IP address
: Most IP addresses can be used as "to" and "from" addresses in packet headers. These are the routable addresses; we expect routing to be possible for them. If we send a packet to one of them, we expect (in most cases; there are various complications) that it will be delivered if the address is in use and will cause an ICMP error packet to come back to us if not.

  There are also several classes on non-routable IP addresses.

RSA algorithm
: Rivest Shamir Adleman public key encryption method, named for its three inventors. Patented (expires in Sept. 2000) with licenses available from RSA Data Security. Widely used.

RSA Data Security
: A company founded by the inventors of the RSA public key algorithm.

SA
: Security Association, the channel negotiated by the higher levels of an IPSEC implementation and used by the lower. SAs are unidirectional; you need a pair of them for two-way communication.

  An SA is defined by three things -- the destination, the protocol (AH orESP) and the SPI, security parameters index. It is used to index other things such as session keys and intialisation vectors.

  For more detail, see our IPSEC Overview and/or RFC 2401.

Secure DNS
: A version of the DNS or Domain Name Service enhanced with authentication services. This is being designed by the IETF DNS security working group. The BIND 8.2 implementation is available for download. Another site has more information.

  IPSEC can use this plus Diffie-Hellman key exchange to bootstrap itself. This would allow opportunistic encryption. Any pair of machines which could authenticate each other via DNS could communicate securely, without either a pre-existing shared secret or a shared PKI.

  Linux FreeS/WAN will support this in a future release.

Secret key cryptography
: See symmetric cryptography

Security Association
: see SA

Sequence number
: A number added to a packet or message which indicates its position in a sequence of packets or messages. This provides some security against replay attacks.

  For automatic keying mode, the IPSEC RFCs require that the sender generate sequence numbers for each packet, but leave it optional whether the receiver does anything with them.

SHA
: Secure Hash Algorithm, a message digest algorithm developed by the NSA for use in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash.

SHA is one of two message digest algorithms available in IPSEC. The other is MD5. Some people do not trust SHA because it was developed by the NSA. There is, as far as we know, no cryptographic evidence that SHA is untrustworthy, but this does not prevent that view from being strongly held.

Signals intelligence (SIGINT)
: Activities of government agencies from various nations aimed at protecting their own communications and reading those of others. Cryptography, cryptanalysis, wiretapping, interception and monitoring of various sorts of signals. The players include the American NSA, British GCHQ and Canadian CSE.

SKIP
: Simple Key management for Internet Protocols, an alternative to IKE developed by Sun and being marketed by their Internet Commerce Group.

Snake oil
: Bogus cryptography. See the Snake Oil FAQ or this paper by Schneier.

SPI
: Security Parameter Index, an index used within IPSEC to keep connections distinct. A Security Association (SA) is defined by destination, protocol and SPI. Without the SPI, two connections to the same gateway using the same protocol could not be distinguished.

For more detail, see our IPSEC Overview and/or RFC 2401.

SSH
: Secure SHell, an encrypting replacement for the insecure Berkeley commands whose names begin with "r" for "remote": rsh, rlogin, etc. Web site.

SSH Communications Security
: A company founded by the authors of SSH. Offices are in Finland and California. They have a toolkit for developers of IPSEC applications.

SSL
: Secure Sockets Layer, a set of encryption and authentication services for web browsers, developed by Netscape. Widely used in Internet commerce. Also known as TLS.

SSLeay
: A free implementation of SSL by Eric Young (eay) and others. Developed in Australia; not subject to US export controls.

Stream cipher
: A symmetric cipher which produces a stream of output which can be combined (often using XOR or bytewise addition) with the plaintext to produce ciphertext. Contrasts with block cipher.

IPSEC does not use stream ciphers. Their main application is link-level encryption, for example of voice, video or data streams on a wire or a radio signal.

subnet
: A group of IP addresses which are logically one network, typically (but not always) assigned to a group of physically connected machines. The range of addresses in a subnet is described using a subnet mask. See next entry.

subnet mask
: A method of indicating the addresses included in a subnet. Here are two equivalent examples:

- 101.101.101.0/24
- 101.101.101.0 with mask 255.255.255.0

The '24' is shorthand for a mask with the top 24 bits one and the rest zero. This is exactly the same as 255.255.255.0 which has three all-ones bytes and one all-zeros byte.

These indicate that, for this range of addresses, the top 24 bits are to be treated as naming a network (often referred to as "the 101.101.101.0/24 subnet") while most combinations of the low 8 bits can be used to designate machines on that network. Two addresses are reserved; 101.101.101.0 refers to the subnet rather than a specific machine while 101.101.101.255 is a broadcast address. 1 to 254 are available for machines.

It is common to find subnets arranged in a hierarchy. For example, a large company might have a /16 subnet and allocate /24 subnets within that to departments. An ISP might have a large subnet and allocate /26 subnets (64 addresses, 62 usable) to business customers and /29 subnets (8 addresses, 6 usable) to residential clients.

S/WAN

Secure Wide Area Network, a project involving RSA Data Security and a number of other companies. The goal is to ensure that all their IPSEC implementations will interoperate so that their customers can communicate with each other securely.

Symmetric cryptography

Symmetric cryptography, also referred to as conventional or secret key cryptography, relies on a *shared secret key*, identical for sender and receiver. Sender encrypts with that key, receiver decrypts with it. The idea is that an eavesdropper without the key be unable to read the messages. There are two main types of symmetric cipher, block ciphers and stream ciphers.

Symmetric cryptography contrasts with public key or asymmetric systems where the two players use different keys.

The great difficulty in symmetric cryptography is, of course, key management. Sender and receiver *must* have identical keys and those keys *must* be kept secret from everyone else. Not too much of a problem if only two people are involved and they can conveniently meet privately or employ a trusted courier. Quite a problem, though, in other circumstances.

It gets much worse if there are many people. An application might be written to use only one key for communication among 100 people, for example, but there would be serious problems. Do you actually trust all of them that much? Do they trust each other that much? Should they? What is at risk if that key is compromised? How are you going to distribute that key to everyone without risking its secrecy? What do you do when one of them leaves the company? Will you even know?

On the other hand, if you need unique keys for every possible connection between a group of 100, then each user must have 99 keys. You need either 99*100/2 = 4950 *secure* key exchanges between users or a central authority that *securely* distributes 100 key packets, each with a different set of 99 keys.

Either of these is possible, though tricky, for 100 users. Either becomes an administrative nightmare for larger numbers. Moreover, keys *must* be changed regularly, so the problem of key distribution comes up again and again. If you use the same key for many messages then an attacker has more text to work with in an attempt to crack that key. Moreover, one successful crack will give him or her the text of all those messages.

In short, the *hardest part of conventional cryptography is key management*. Today the standard solution is to build a hybrid system using public key techniques to manage keys.

TIS

Trusted Information Systems, a firewall vendor now part of NAI. Their Gauntlet product offers IPSEC VPN services. TIS implemented the first version of Secure DNS on a DARPA contract.

TLS
: Transport Layer Security, a newer name for SSL.

Traffic analysis
: Deducing useful intelligence from patterns of message traffic, without breaking codes or reading the messages. In one case during World War II, the British knew an attack was coming because all German radio traffic stopped. The "radio silence" order, intended to preserve security, actually gave the game away.

In an industrial espionage situation, one might deduce something interesting just by knowing that company A and company B were talking, especially if one were able to tell which departments were involved, or if one already knew that A was looking for acquisitions and B was seeking funds for expansion.

IPSEC itself does not defend against this, but carefully thought out systems using IPSEC can do so. In particular, one might want to encrypt more traffic than was strictly necessary, route things in odd ways, or even encrypt dummy packets, to confuse the analyst.

Transport mode
: An IPSEC application in which the IPSEC gateway is the destination of the protected packets, a machine acts as its own gateway. Contrast with tunnel mode.

Triple DES
: see 3DES

Tunnel mode
: An IPSEC application in which an IPSEC gateway provides protection for packets to and from other systems. Contrast with transport mode.

Two-key Triple DES
: A variant of triple DES or 3DES in which only two keys are used. As in the three-key version, the order of operations is EDE or encrypt-decrypt-encrypt, but in the two-key variant the first and third keys are the same.

3DES with three keys has 3*56 = 168 bits of key but has only 112-bit strength against a meet-in-the-middle attack, so it is possible that the two key version is just as strong. Last I looked, this was an open question in the research literature.

RFC 2451 defines triple DES for IPSEC as the three-key variant. The two-key variant should not be used and is not implemented directly in Linux FreeS/WAN. It cannot be used in automatically keyed mode without major fiddles in the source code. For manually keyed connections, you could make Linux FreeS/WAN talk to a two-key implementation by setting two keys the same in /etc/ipsec.conf.

Virtual Interface
: A Linux feature which allows one physical network interface to have two or more IP addresses. See the *Linux Network Administrator's Guide* in book form or on the web for details.

Virtual Private Network
: see VPN

VPN
: Virtual Private Network, a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.

IPSEC is not the only technique available for building VPNs, but it is the only method defined by RFCs and supported by many vendors. VPNs are by no means the only thing you can do with IPSEC, but they may be the most important application for many users.

VPNC
: Virtual Private Network Consortium, an association of vendors of VPN products.

Wassenaar Arrangement
: An international agreement restricting export of munitions and other tools of war. Unfortunately, cryptographic software is also restricted under the current version of the agreement.

Web of Trust
: PGP's method of certifying keys. Any user can sign a key; you decide which signatures or combinations of signatures to accept as certification. This contrasts with the hierarchy of CAs (Certification Authorities) used in many PKIs (Public Key Infrastructures).

  See Global Trust Register for an interesting addition to the web of trust.

X.509
: A standard from the ITU (International Telecommunication Union), for hierarchical directories with authentication services, used in many PKI implementations.

  Use of X.509 services, via the LDAP protocol, for certification of keys is allowed but not required by the IPSEC RFCs. It is not yet implemented in Linux FreeS/WAN.

Xedia
: A vendor of router and Internet access products. Their QVPN products interoperate with Linux FreeS/WAN; see our compatibility document.

Click below to go to:

- Document index file
- Table of Contents
- Beginning of this file
- FreeS/WAN home page

OIPE JC98
JUN 1 3 2002
PATENT & TRADEMARK OFFICE

#11/D
mm
6-26-02

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
JUN 2 4 2002
Technology Center 2100

In Re Application Of	
Edmund Colby MUNGER *et al.*	
Serial No.:	09/504,783
Filed:	February 15, 2000
For:	IMPROVEMENTS TO AN AGILE NETWORK PROTOCOL FOR SECURE COMMUINCATIONS WITH ASSURED SYSTEM AVAILABILITY

Group Art Unit: 2153

Examiner: K. Lim

Atty. Dkt. No. 00479.85672

AMENDMENT AND RESPONSE UNDER 37 C.F.R. § 1.111

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In response to the Office Action mailed March 13, 2002, Applicants respectfully request the application be amended as follows. No fee is believed to be due with this Request. However, if a fee is due the Office is authorized to charge any required fees for consideration of this paper to our Deposit Account No. 19-0733.

IN THE CLAIMS

Please cancel claims 72-81.

Remarks

Applicants are in receipt of the Office Action mailed March 13, 2002, indicating that claims 28-39 and 67-81 are pending, claims 72-81 are withdrawn from consideration, claims 28-37 and 67-

, 69 stand rejected, and claims 38, 39, 70 and 71 are objected to. Applicants thank the Examiner for the indication of allowable subject matter in claims 38, 39, 70, and 71.

Submitted concurrently herewith are formal drawings in substitution for the informal drawings submitted with the application as filed. Applicants respectfully request that the official draftsman reviews the formal drawings at his earliest convenience.

Second Preliminary Amendment and IDS

A Second Preliminary Amendment adding claims 82-91 was submitted on February 22, 2002, but this amendment was not reflected in the Office Action mailed on March 13, 2002. Applicants respectfully request that the Second Preliminary Amendment be entered as of the date of its receipt by the Office, and that the claims submitted in the Second Preliminary Amendment be considered simultaneously with the requested reconsideration of the pending claims.

A Supplemental Information Disclosure Statement was also submitted February 22, 2002, but was not reflected in the Office Action mailed on March 13, 2002. Applicants respectfully request that the references cited in the Supplemental Information Disclosure Statement be considered and acknowledged at the Examiner's earliest convenience.

On the Merits

The Office Action restricted newly added claims 72-81 (group IV) as being drawn to an independent or distinct invention from the originally claimed invention in claims 28-39 and 67-71 (group II), and constructively elected group II for prosecution on the merits. By the present amendment, Applicants cancel claims 72-81.

The Office Action rejected claims 28-37 and 67-69 under 35 U.S.C. § 103(a) as being unpatentable over *Boden et al.* (U.S. Pat. No. 6,330,562, hereinafter "Boden") in view of *Risley et al.* (U.S. Pat. No. 6,332,158, hereinafter "Risley"). Applicants respectfully traverse this rejection based on the following arguments.

In order to reject a claim as obvious under § 103(a), three criteria must exist: 1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combined reference teachings; 2) there must be a reasonable expectation of success; and 3) the prior art reference(s) must teach or suggest all the claim limitations. See MPEP § 706.02 (j); *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991).

First, Applicants submit that there is no motivation or suggestion to combine the Boden and Risley references. Boden discloses a data model for abstracting customer-defined VPN security policy information (Boden, Abstract). The system in Boden addresses the need to enable connection filter rules to be generated and loaded dynamically at negotiation time, due to remote initiating hosts having *dynamically assigned IP addresses*. Boden, col. 2, lines 38-41 (emphasis added). As cited in the Office Action, Boden allows for "dynamically establishing VPN connections with different security policies and other attributes, based solely on an unfixed IP address (e.g. [sic] *a user ID*)...." Boden, col. 3, lines 14-16 (emphasis added). Boden does not disclose establishing a VPN based on a DNS request for an IP address.

Risley discloses a DNS lookup system that allows intelligent correction of domain name searches by providing alternative suggestions of possible intended domain names when a DNS lookup was unsuccessful. Risley, Abstract. That is, when a user submits a domain name query, if the domain name exists, the domain name server (DNS) provides the corresponding machine address back to the user, as is known in the art. However, if the domain name does not exist, the Risley domain name server returns a machine address for a machine that will help the user identify the desired domain name. Subsequently, the machine to which the user has been redirected suggests possible intended domain names based on heuristics such as common misspellings, phonetic errors, and the like. Risley, Abstract. Risley does not teach or suggest establishing a VPN based on a DNS request, nor establishing any sort of secure communications channel over a network.

The Office Action states that establishing a secure connection between computers with the use of VPN would have been a desired feature in the art as suggested by Boden at col. 1, lines 41-55. However, Boden at col. 1, lines 41-55, discusses a general need for computer security, not a specific suggestion to incorporate the VPN techniques disclosed in Boden, or any other security technique, with a DNS lookup assistant as disclosed by Risley. In addition, there are many ways in which to create a VPN, and Boden at best only discloses a single specific security solution that may be used to establish a VPN. Boden does not include any suggestion or motivation to alter a DNS request scheme to create a VPN (in fact, there is only one instance of the acronym DNS in the entire Boden specification, col. 10, line 3, and no instances of the phrase "domain name service"). Indeed, Boden specifically states that "no verification is made via DNS or similar that [the mapping of ID to IP address] is correct." *Id.*

The Office Action also states that "the system that made it easier to remember, access, and convey the location information in order to access information would have been also a desired feature in the art as suggested by [Risley col. 1, lines 46-52]." However, Risley at col. 1, lines 46-52, discusses the general notion that users prefer using domain names (e.g., coolsite.com) rather than IP addresses (e.g., 199.227.249.232) when remembering, accessing, and conveying information. Risley does not provide a specific suggestion that its DNS service would benefit from the use of a VPN (or any other type of security). Risley only discloses that users prefer to use domain names over IP addresses when remembering, accessing, and conveying information, and provides a system for helping a user identify an intended domain name.

The Office Action concludes that it would have been obvious to combine the references in order to have "an easier to use and secure network connection because the teachings of these two references are complemented each other for easier to use and for securing network connection in a computer network." While two patents may ostensibly complement each other, this does not provide the necessary suggestion to combine the two references. In light of the fact that neither reference includes a specific suggestion to combine the references, the mere fact that two references are complementary does not provide the required suggestion or motivation. Risley does not teach or suggest establishing a VPN using its domain name resolution technique, nor does Boden teach using domain name resolution to establish a VPN.

To allow the combination of Boden and Risley would allow the hindsight combination of almost any two references as long as they had something in common, e.g., they both relate to the Internet. The Federal Circuit has repeatedly stated that the limitations of a claim in a pending application cannot be used as a blueprint to piece together prior art in hindsight, *In re Dembiczak*, 50 U.S.P.Q.2d 1614 (Fed. Cir. 1999), and that the Patent Office should *rigorously* apply the requirement that a teaching or motivation to combine prior art references needs to be provided. *Id.* (emphasis added). Thus, Applicants respectfully submit that that there is no motivation or suggestion to combine Risley, which discloses a modified DNS lookup system, with Boden, which discloses a specific VPN technique.

Second, even if the Boden and Risley references were combined, the combination would not teach or suggest all the limitations of any pending claim. The Office Action uses claim 37 as an exemplary claim, which requires:

> a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested; and
>
> a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server.

At a minimum, neither Boden nor Risley discloses a DNS proxy server that "generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested..." Neither Risley nor Boden teach or suggest triggering the creation of a VPN in response to a DNS request. Instead, Risley discloses a modified DNS lookup, whereby when a DNS request is received that is unsuccessful, Risley redirects the requestor to a domain name resolver to assist the user with locating an intended domain name. Risley does not disclose generating a request to create a VPN, as is required by claim 37, nor does Risley determine whether access to a secure web site has been requested. Likewise, Boden does not disclose these limitation, as is admitted in the Office Action at page 5, para. 11.

In addition, the Office Action does not indicate that either Boden or Risley includes a gatekeeper computer as is required by claim 37.

Based at least on the above arguments, Applicants respectfully traverse the rejection of claim 37 and its dependent claims.

The Office Action also rejected claims 28-36 and 67-69 for the same reasons set forth with respect to claim 37 because the claims are similar in scope. Applicants submit that each claim presents an individually patentable scope, and that these claims are allowable for at least the same reasons as claim 37.

In addition, with respect to claim 31, none of the cited references teach or suggest, upon determining that a client computer is not authorized to establish a VPN with a secure web site, returning an error from the DNS request.

With respect to claim 32, none of the cited references teach or suggest, upon determining that a client computer is not authorized to resolve addresses of non-secure target computers, returning an error from the DNS request.

With respect to claim 33, none of the cited references teach or suggest establishing the VPN by creating an IP address hopping scheme between the client computer and the target computer. (see, e.g., allowable subject matter in claim 38).

With respect to claim 34, none of the cited references teach or suggest using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer.

With respect to claim 35, none of the cited references teach or suggest that step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site.

With respect to claim 68, none of the cited references teach or suggest communicating according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence.

With respect to claim 69, none of the cited references teach or suggest comparing an Internet Protocol (IP) address in a header of each data packet to a table of valid IP addresses maintained in a table in the second computer.

Based on the aforementioned Applicants respectfully submit that all pending claims are in condition for allowance, and Applicants request that the subject application be reconsidered and passed to issue at the Examiner's earliest possible convenience.

If the Examiner has any questions or wishes to discuss this amendment, the Examiner is invited to telephone the undersigned representative at the number set forth below.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Date: June 13, 2002 By: ____________________

Bradley C. Wright Reg. No. 49,024
Registration No. 38,061
1001 G Street N.W., 11th Floor
Washington, D.C. 20001
(202) 508-9100

2153

JUN 1 3 2002 PATENT & TRADEMARK OFFICE

PTO/SB/21 (08-00)

Please type a plus sign (+) inside this box ---> [+]

Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/504,783
Filing Date	February 15, 2000
First Named Inventor	Edmund Colby Munger
Group Art Unit	2153
Examiner Name	K. Lim
Attorney Docket Number	000479.85672
Total Number of Pages in This Submission	

RECEIVED JUN 2 4 2002 Technology Center 2100

ENCLOSURES *(check all that apply)*

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [x] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Assignment Papers *(for an Application)*
- [x] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ______
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) *(please identify below):*

  Submission of Formal Drawings to Official Draftsman

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Bradley C. Wright, Reg. No. 38,061
Signature	Ross D... **Reg. No. 49,024**
Date	June 13, 2002

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on this date: ______

Typed or printed name			
Signature		Date	

JUN 1 2002 PATENT & TRADEMARK OFFICE

#9
#12

PATENT APPLICATION

RECEIVED
JUN 2 4 2002
Technology Center 2100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Edmond Colby Munger et al.

Serial No. 09/504,783

Filed: February 15, 2000

Group Art Unit: 2153

Examiner: K. Lim

Attorney Docket No. 00479.85672

For: IMPROVEMENTS TO AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

SUBMISSION OF FORMAL DRAWINGS TO OFFICIAL DRAFTSMAN

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Please substitute the attached 35 sheets of formal drawings depicting Figures 1-32 for the informal drawings filed with the patent application on February 15, 2000, in this matter. Applicant respectfully requests the Official Draftsman to review these drawings and advise the undersigned of any objections thereto.

It is believed that no fee is required. However, if a fee is required, please charge our Deposit Account No. 19-0733.

Respectfully submitted,

Date: June 13, 2002

By: Ross Dannenberg
for Bradley C. Wright
Registration No. 38,061 **Reg. No. 49,024**

BANNER & WITCOFF, LTD
1001 G Street, N.W.
Eleventh Floor
Washington, D.C. 20001
(202) 508-9100
RAD/mmd

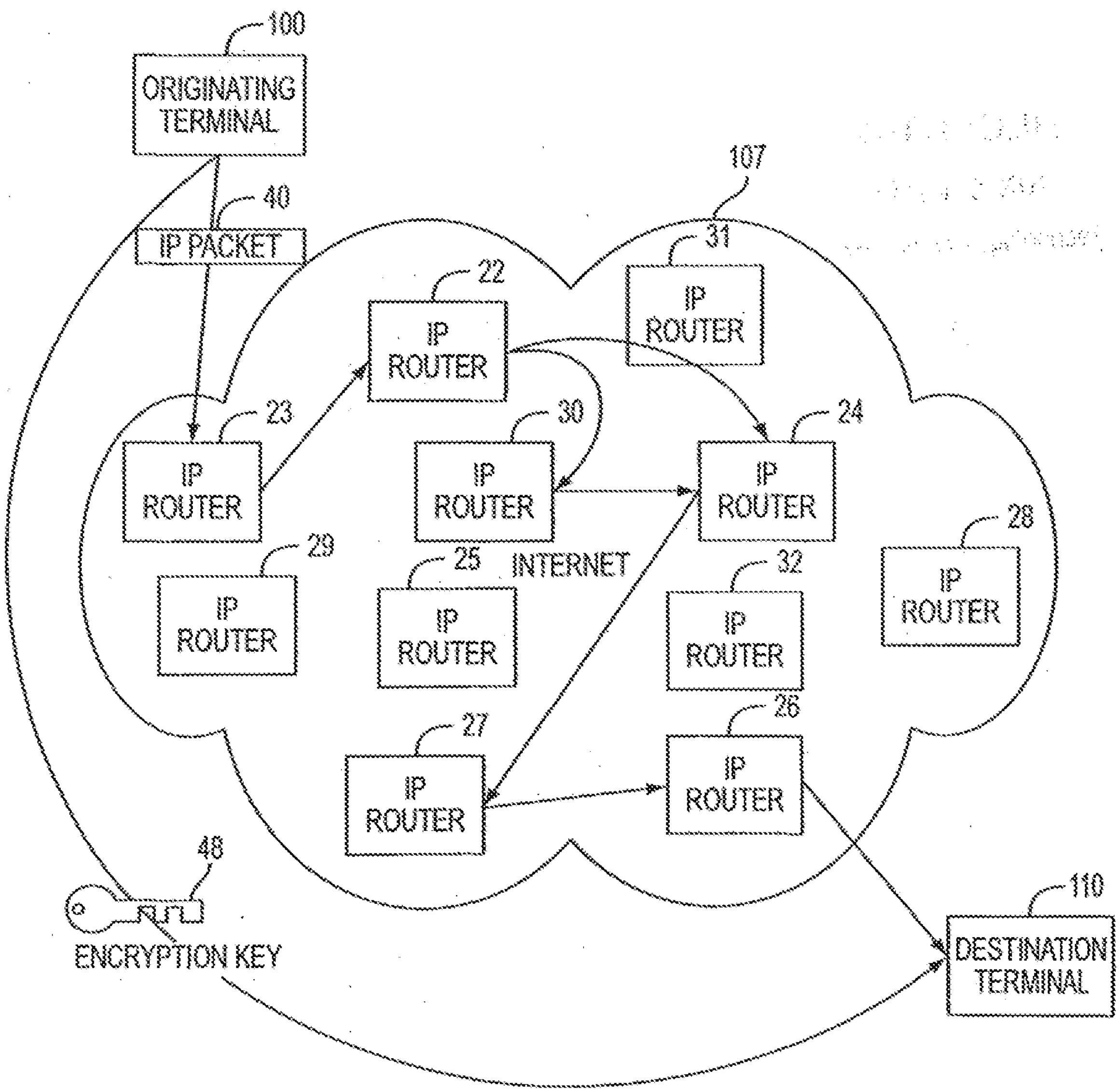

100
ORIGINATING TERMINAL
40
IP PACKET
107
31
IP ROUTER
22
IP ROUTER
23
IP ROUTER
30
IP ROUTER
24
IP ROUTER
28
IP ROUTER
29
IP ROUTER
25
IP ROUTER
INTERNET
32
IP ROUTER
27
IP ROUTER
26
IP ROUTER
48
ENCRYPTION KEY
110
DESTINATION TERMINAL

FIG. 1

OIPE JC99
JUN 1 3 2002
PATENT & TRADEMARK OFFICE

RECEIVED
JUN 2 4 2002
Technology Center 2100

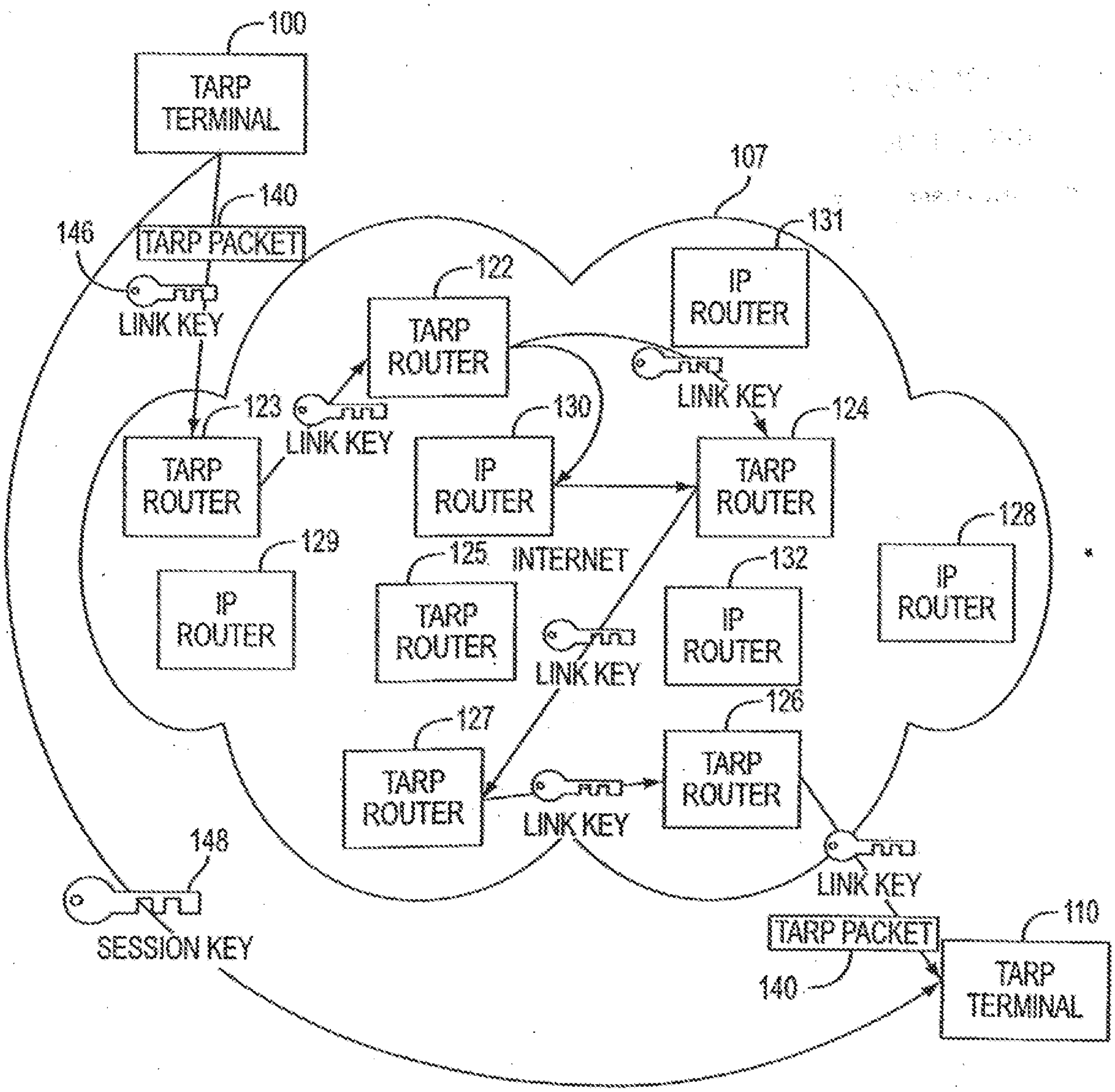

100
TARP TERMINAL
107
140
TARP PACKET
146
LINK KEY
131
IP ROUTER
122
TARP ROUTER
LINK KEY
123
LINK KEY
130
124
TARP ROUTER
IP ROUTER
TARP ROUTER
128
129
IP ROUTER
125
INTERNET
132
IP ROUTER
TARP ROUTER
IP ROUTER
LINK KEY
127
126
TARP ROUTER
TARP ROUTER
LINK KEY
148
LINK KEY
SESSION KEY
TARP PACKET
110
140
TARP TERMINAL

FIG. 2

OIPE JCGO
JUN 1 3 2002
PATENT & TRADEMARK OFFICE

RECEIVED
JUN 2 4 2002
Technology Center 2100

VNET00221433

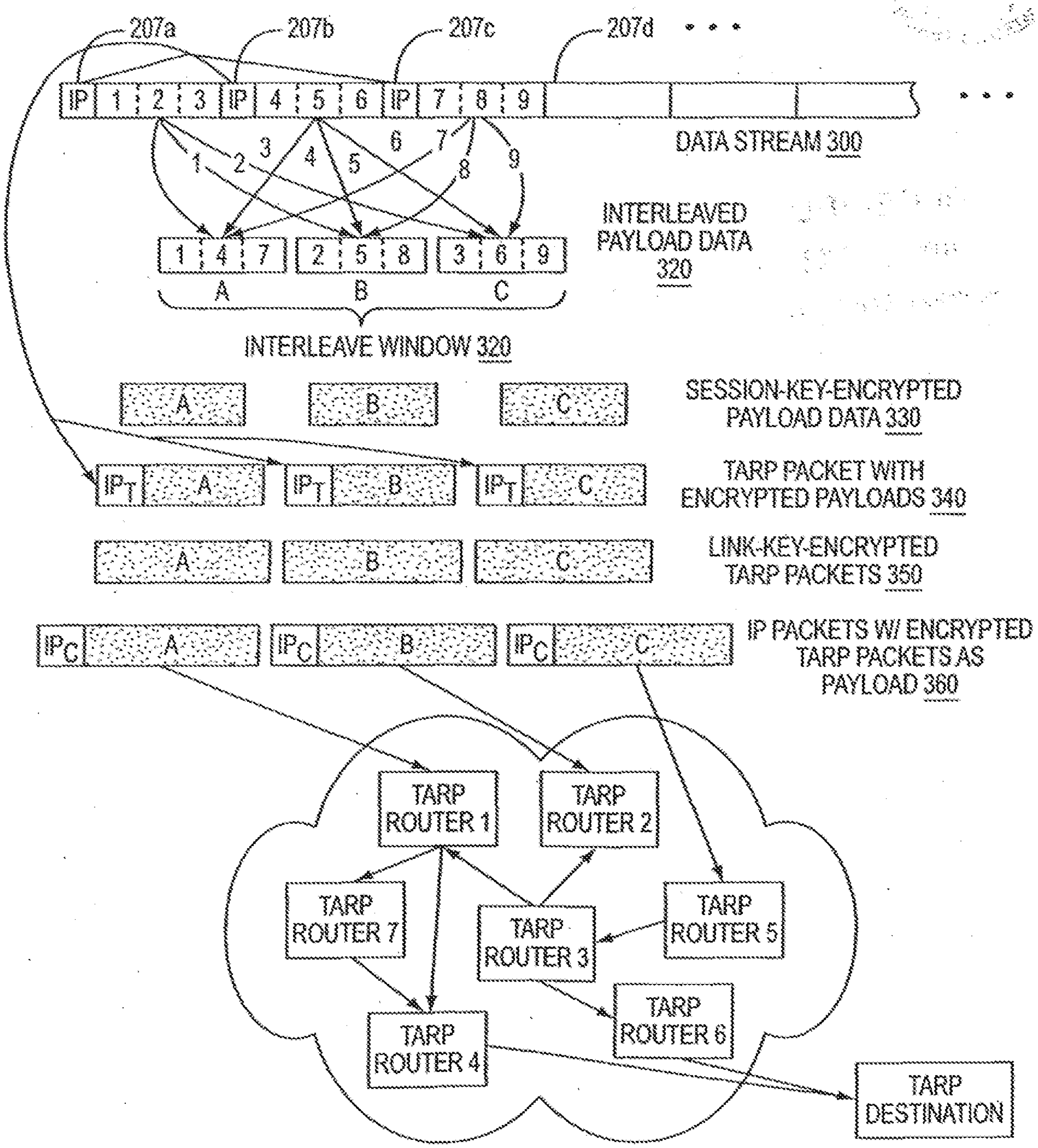
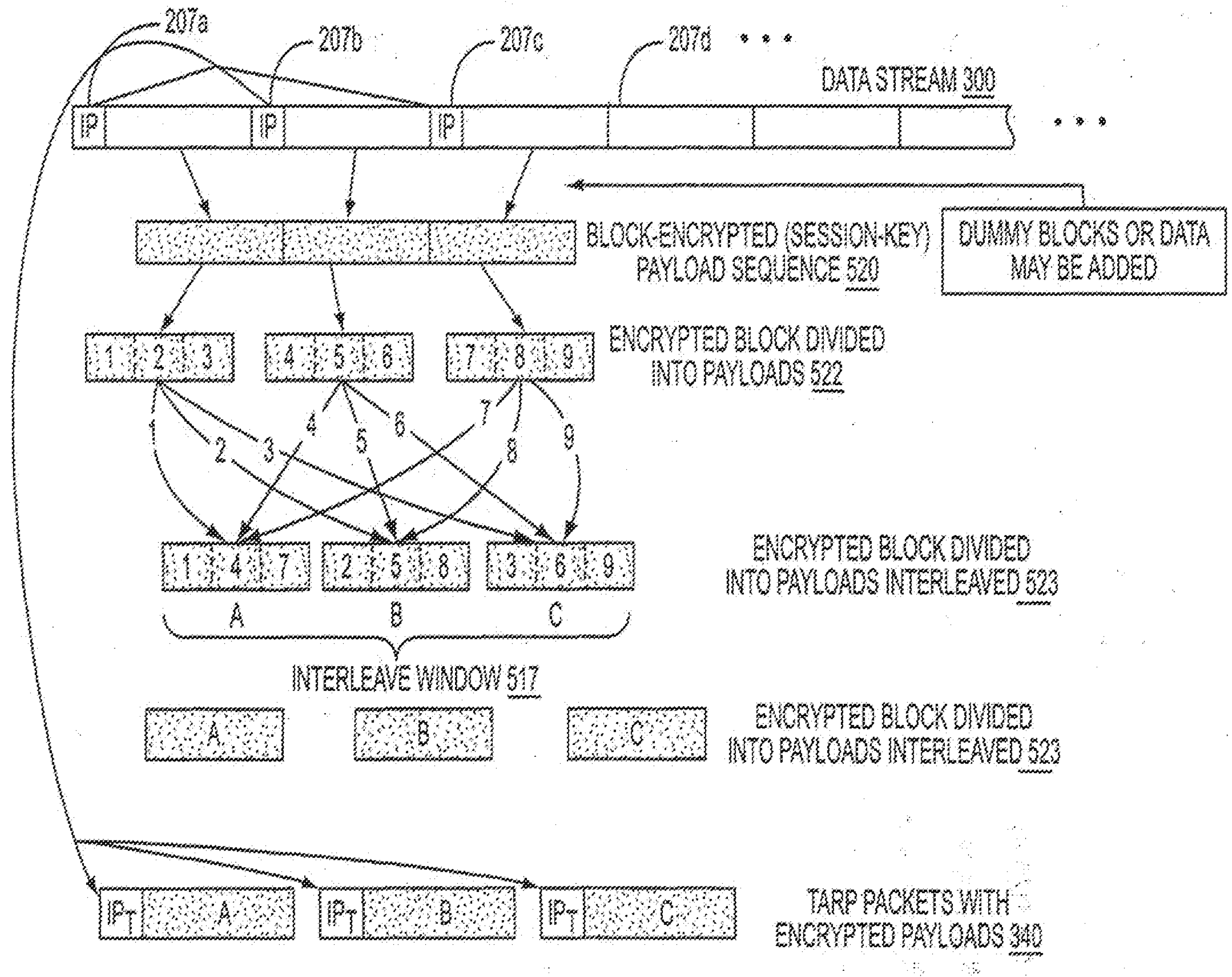

207a
207b
207c
207d
IP
1
2
3
IP
4
5
6
IP
7
8
9
DATA STREAM 300
INTERLEAVED PAYLOAD DATA 320
1 4 7
2 5 8
3 6 9
A
B
C
INTERLEAVE WINDOW 320
SESSION-KEY-ENCRYPTED PAYLOAD DATA 330
TARP PACKET WITH ENCRYPTED PAYLOADS 340
LINK-KEY-ENCRYPTED TARP PACKETS 350
IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD 360
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 6
TARP ROUTER 4
TARP DESTINATION

FIG. 3A

OIPE JC99
JUN 13 2002
PATENT & TRADEMARK OFFICE

RECEIVED
JUN 24 2002
Technology Center 2100

VNET00221435



207a
207b
207c
207d
DATA STREAM 300
IP
IP
IP
BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE 520
DUMMY BLOCKS OR DATA MAY BE ADDED
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS 522
1 2 3
4 5 6
7 8 9
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED 523
1 4 7
2 5 8
3 6 9
A
B
C
INTERLEAVE WINDOW 517
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED 523
TARP PACKETS WITH ENCRYPTED PAYLOADS 340

FIG. 3B

OIPE
JUN 1 3 2002
PATENT & TRADEMARK OFFICE

RECEIVED
JUN 2 4 2002
Technology Center 2100

VNET00221437

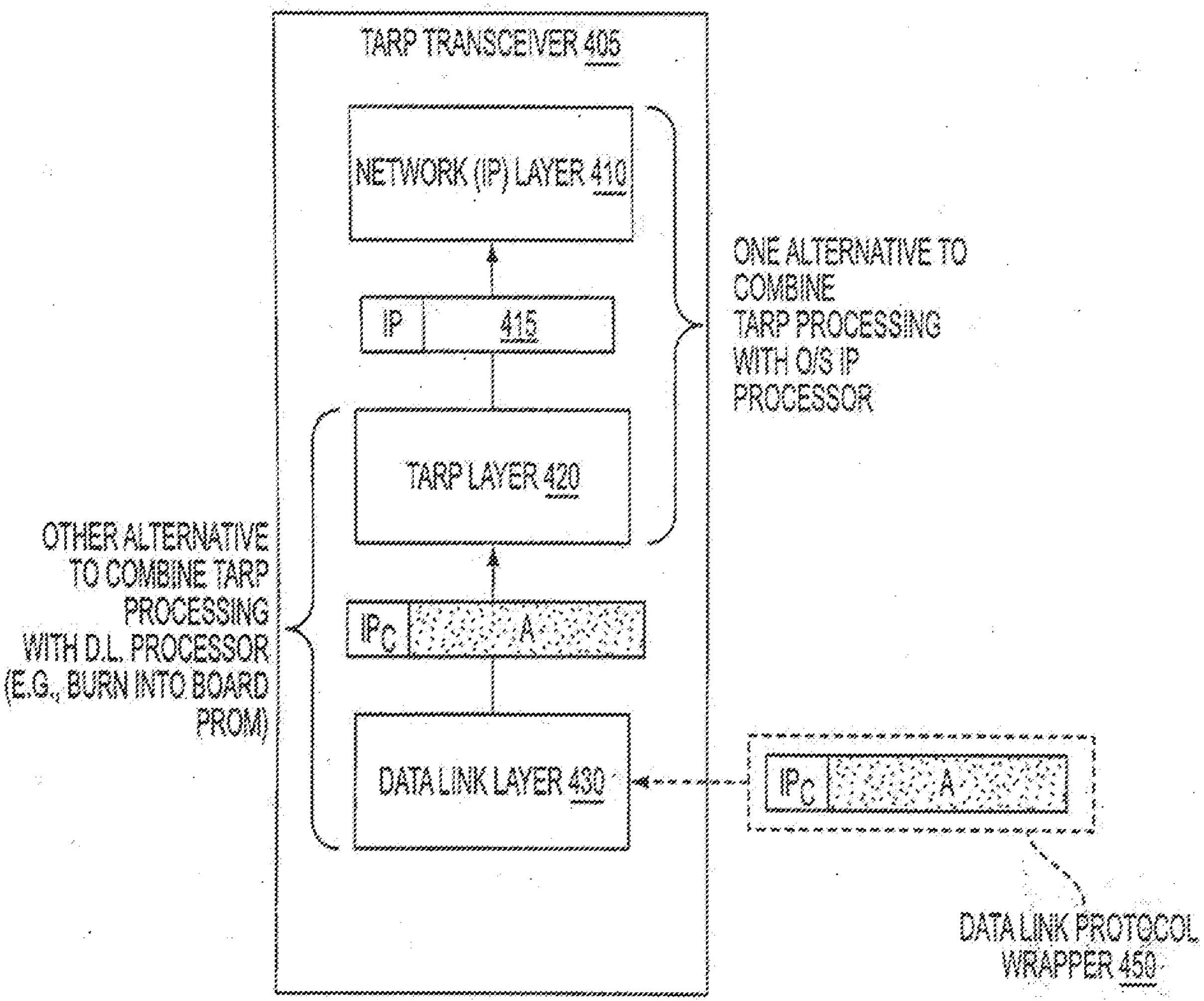

TARP TRANSCEIVER 405
NETWORK (IP) LAYER 410
IP
415
TARP LAYER 420
IPC
A
DATA LINK LAYER 430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (E.G., BURN INTO BOARD PROM)
IPC
A
DATA LINK PROTOCOL WRAPPER 450

FIG. 4

3. The method as defined by claim 2, wherein said key K_{ij} is derived from $\propto^{ij}$ mod p using low order key-size bits of $\propto^{ij}$ mod p.

4. The method as defined by claim 3, wherein the key K_{ij} is an implicit pair-wise shared secret used as a key for a shared key cryptosystem (SKCS).

5. The method as defined by claim 4, wherein said SKCS is DES.

6. The method as defined by claim 5, wherein said SKCS is RC2.

7. The method as defined by claim 4, wherein said data packet includes a source address, a destination address and an SKCS identifier field.

8. The method as defined by claim 7, wherein said data packet further includes a message indicator field.

9. The method as defined by claim 4, wherein $\propto$ and p are system parameters, and where p is a prime number.

10. An apparatus for encrypting data for transmission from a first data processing device (node I) to a second data processing device (node J), comprising:

node I including a first storage device for storing a secret value i, and a public value $\propto^{i}$ mod p;

node J including a second storage device for storing a secret value j, and a public value $\propto^{j}$ mod p;

node I including an encrypting device for encrypting a data packet to be transmitted to node J, said data packet being encrypted using a first Diffie-Helman (DH) certificate for node J to determine said public value $\propto^{j}$ mod p;

said encrypting device further computing the value of $\propto^{ij}$ mod p and deriving a key K_{ij} from said value $\propto^{ij}$ mod p;

said encrypting device encrypting a randomly generated transient key K_p from K_{ij}, and encrypting said data packet using said transient key K_p;

node I further including an interface circuit for transmitting said encrypted data packet to said node J.

11. The apparatus as defined by claim 10, wherein said node J further includes:

a receiver for receiving said encrypted data packet from node I;

a decrypting device coupled to said receiver for decrypting said data packet from node I.

12. The apparatus as defined by claim 11, wherein said decrypting device obtains a second DH certificate for said node I and determines said public value $\propto^{i}$ mod p, and computes the value of $\propto^{ij}$ mod p, said decrypting device further deriving said key K_{ij} from $\propto^{ij}$ mod p.

13. The apparatus as defined by claim 12, wherein said decrypting device utilizes said key K_{ij} to decrypt said transient key K_p, and decrypts said received data packet using said transient key K_p.

14. The apparatus as defined by claim 13, wherein said key K_{ij} is derived from $\propto^{ij}$ mod p using low order key-size bits of $\propto^{ij}$ mod p.

15. The apparatus as defined by claim 14, wherein said key K_{ij} is an implicit pair-wise shared secret used as a key for a shared key cryptosystem (SKCS).

16. The apparatus as defined by claim 15, wherein said data packet includes a source address, a destination address and an SKCS identifier field.

17. The apparatus as defined by claim 16, wherein said data packet further includes a message indicator field.

18. The apparatus as defined by claim 17, wherein $\propto$ and p are system parameters, and where p is a prime number.

19. The apparatus as defined by claim 15, wherein said SKCS is DES.

20. The apparatus as defined by claim 15, where said SKCS is RC2.

* * * * *

US005689566A

United States Patent [19]

Nguyen

[11] **Patent Number:** 5,689,566

[45] **Date of Patent:** Nov. 18, 1997

[54] **NETWORK WITH SECURE COMMUNICATIONS SESSIONS**

[76] Inventor: Minhtam C. Nguyen, 10018 Lexington Estates Blvd., Boca Raton, Fla. 33428

[21] Appl. No.: **547,346**

[22] Filed: **Oct. 24, 1995**

[51] **Int. Cl.**^{6} **H04K 1/00**

[52] **U.S. Cl.** **380/25**; 380/29; 380/49

[58] **Field of Search** 380/25, 23, 24, 380/4, 46, 49, 29

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,227,253	10/1980	Ehrsam et al.	375/2
5,060,263	10/1991	Bosen et al.	380/25
5,073,852	12/1991	Siegel et al.	395/700
5,111,504	5/1992	Esserman et al.	380/21
5,136,716	8/1992	Harvey et al.	395/800
5,142,622	8/1992	Owens	395/200
5,220,655	6/1993	Tsutsui	395/325
5,226,172	7/1993	Seymour et al.	395/800
5,239,648	8/1993	Nukui	395/600
5,241,599	8/1993	Bellovin et al.	380/21
5,261,070	11/1993	Ohta	395/425
5,263,165	11/1993	Janis	395/725
5,268,962	12/1993	Abadi et al.	380/21
5,301,247	4/1994	Rasmussen et al.	380/43
5,311,593	5/1994	Carmi	380/23
5,323,146	6/1994	Glaschick	340/825.34
5,369,707	11/1994	Follendore, III	380/25
5,373,559	12/1994	Kaufman et al.	380/30
5,375,207	12/1994	Blakely et al.	395/200
5,392,357	2/1995	Bulfer et al.	380/33
5,416,842	5/1995	Aziz	380/30
5,418,854	5/1995	Kaufman et al.	380/23

OTHER PUBLICATIONS

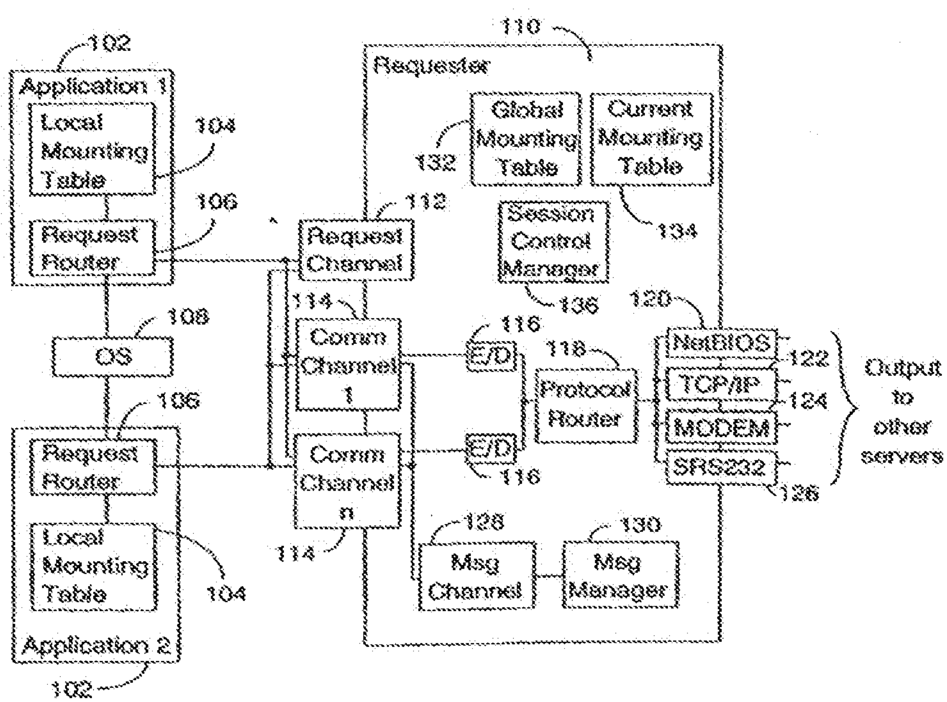
Bruce Schneier, *Applied Cryptography* (second edition), New York, NY, John Wiley & Sons, Inc. 1996, pp. 298–301.

Primary Examiner—David C. Cain
Attorney, Agent, or Firm—John C. Smith

[57] **ABSTRACT**

A system which uses three way password authentication, encrypting different portions of a logon packet with different keys based on the nature of the communications link. Nodes attached to a particular LAN can have one level of security for data transfer within the LAN while data transfers between LANs on a private network can have a second level of security and LANs connected via public networks can have a third level of security. The level of security can optionally be selected by the user. Data transfers between nodes of a network are kept in separate queues to reduce queue search times and enhance performance.

20 Claims, 13 Drawing Sheets



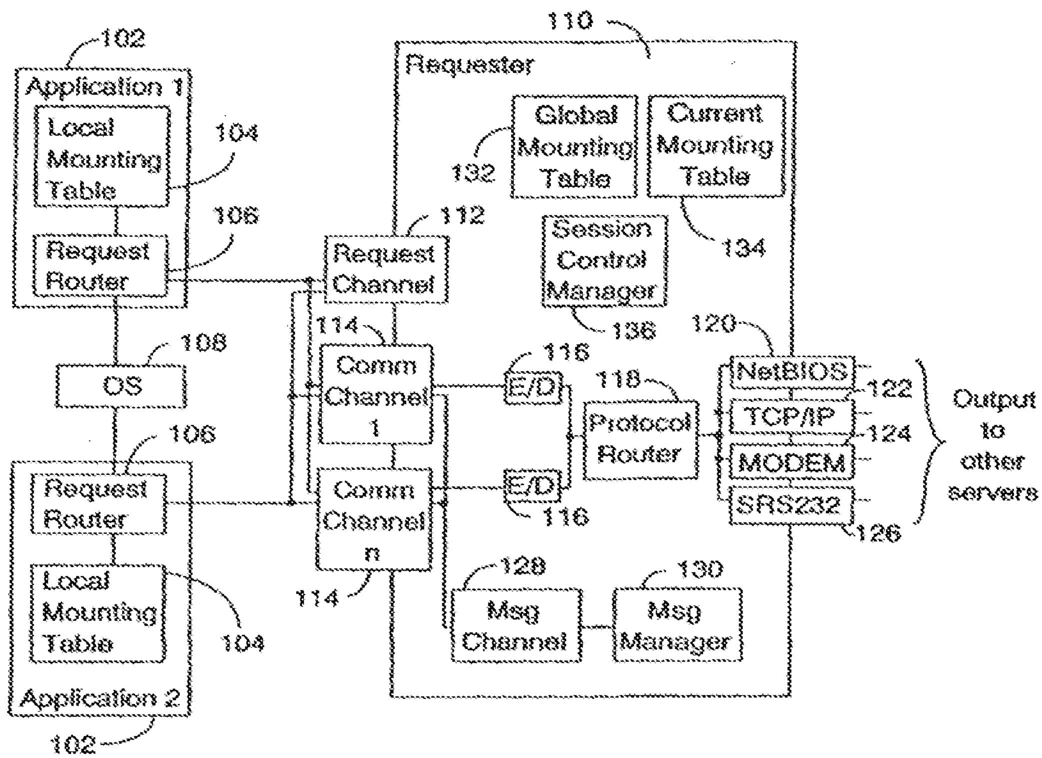
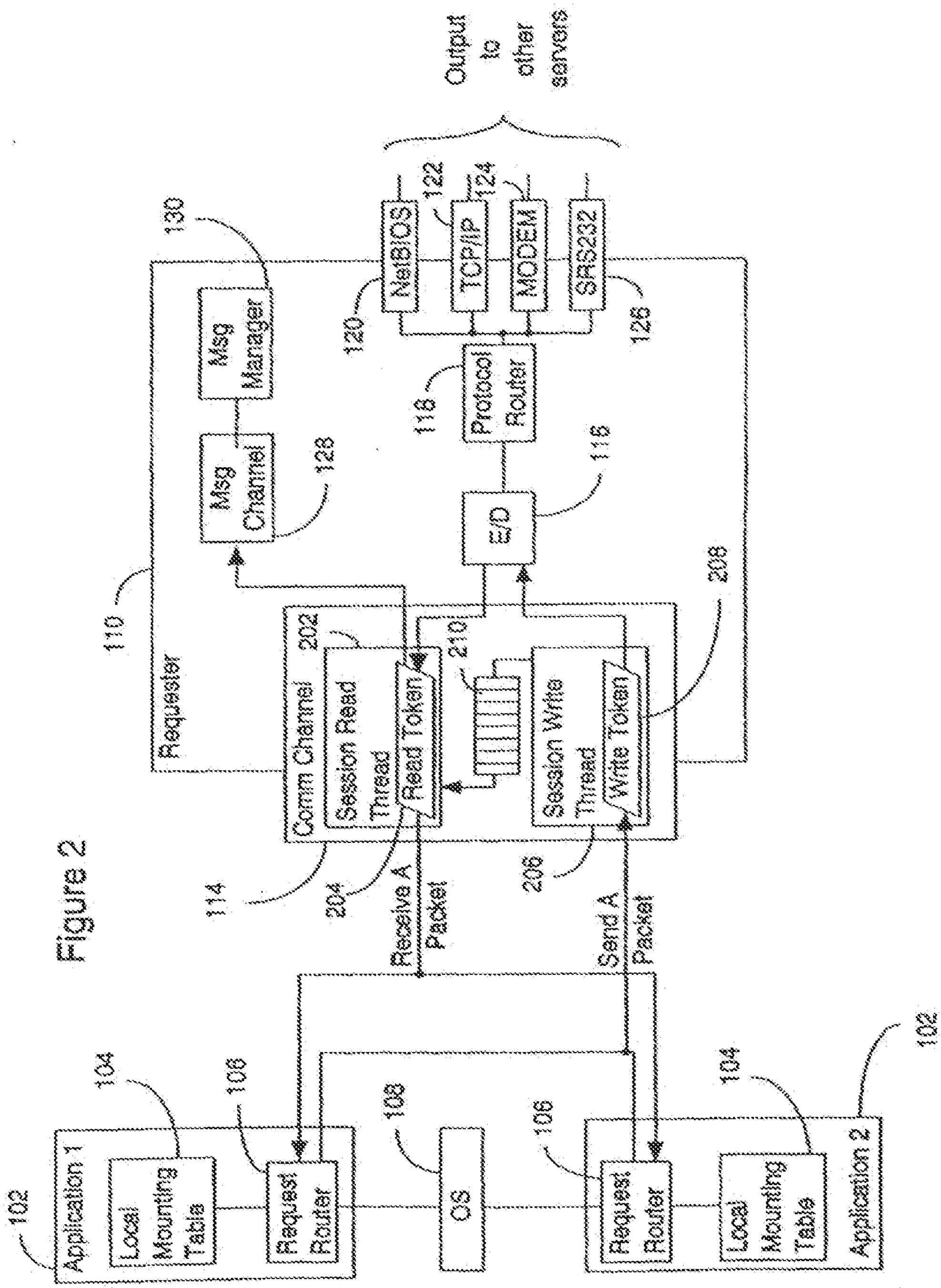

110
Requester
102
Application 1
Local Mounting Table
104
106
Request Router
Global Mounting Table
Current Mounting Table
132
134
112
Request Channel
Session Control Manager
136
108
OS
114
Comm Channel 1
116
E/D
118
Protocol Router
120
NetBIOS
122
TCP/IP
124
MODEM
SRS232
126
Output to other servers
106
Request Router
Local Mounting Table
104
Comm Channel n
E/D
116
114
128
Msg Channel
130
Msg Manager
Application 2
102

Figure 1


Output
to
other
servers
130
122
124
NetBIOS
TCP/IP
MODEM
SRS232
120
126
Msg
Manager
Protocol
Router
118
Msg
Channel
128
E/D
116
110
Requester
208
202
210
Comm Channel
Session Read
Thread
Read Token
Session Write
Thread
Write Token
114
204
206
Receive A
Packet
Send A
Packet
104
106
108
106
104
102
Application 1
Local
Mounting
Table
Request
Router
OS
Request
Router
Local
Mounting
Table
Application 2
102
Figure 2

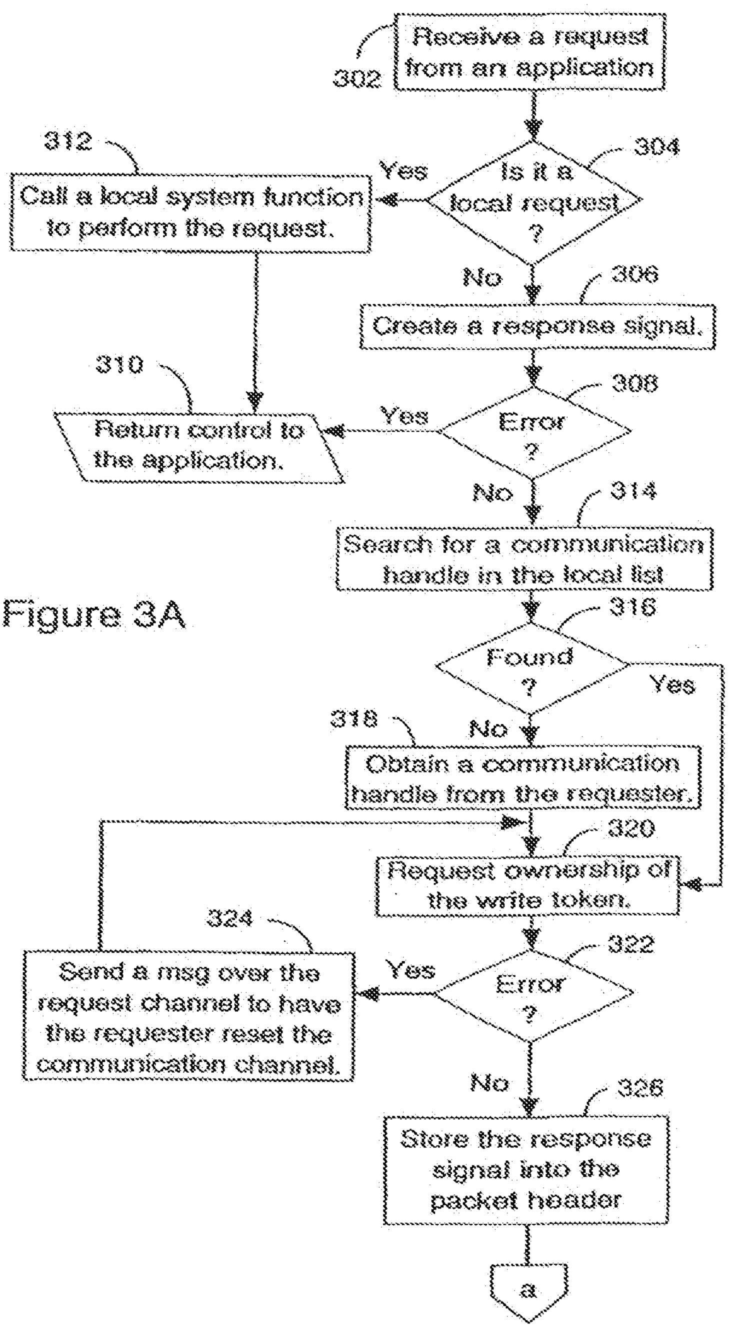
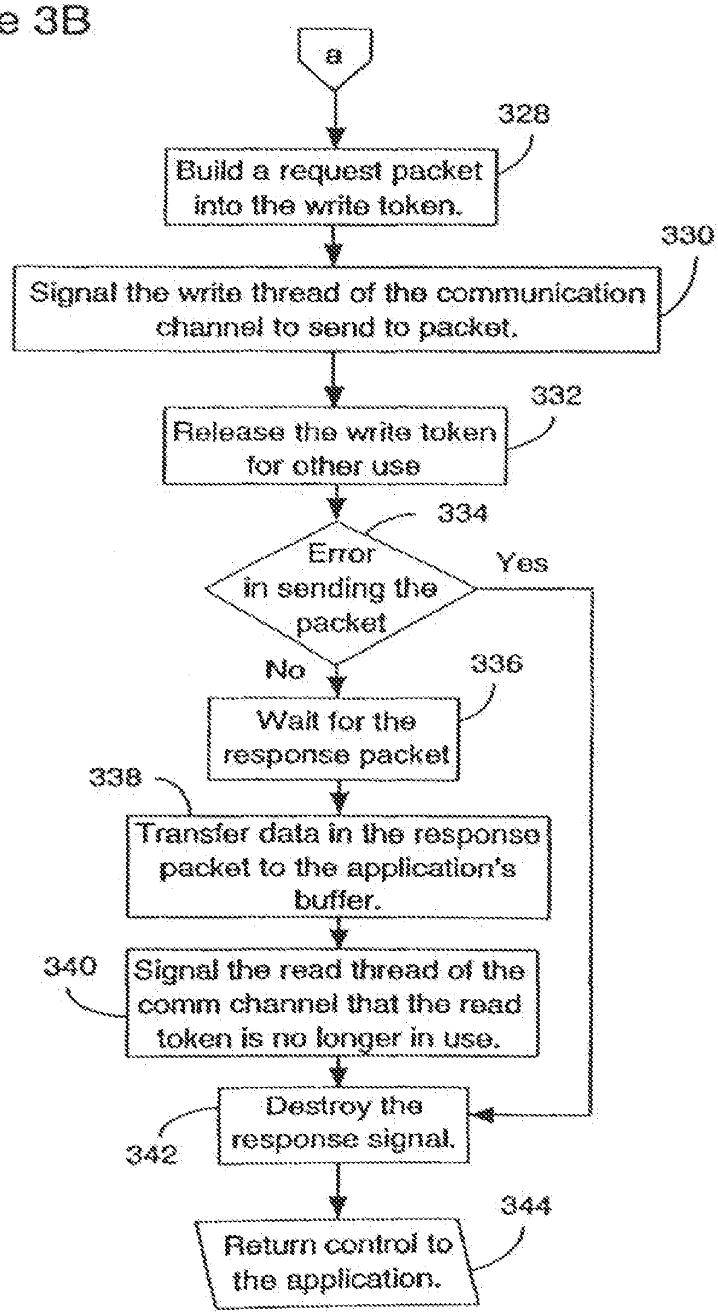

Receive a request from an application
302
Is it a local request ?
304
Yes
312
Call a local system function to perform the request.
No
306
Create a response signal.
310
Return control to the application.
Yes
Error ?
308
No
314
Search for a communication handle in the local list
316
Found ?
Yes
318
No
Obtain a communication handle from the requester.
320
Request ownership of the write token.
324
Send a msg over the request channel to have the requester reset the communication channel.
Yes
Error ?
322
No
326
Store the response signal into the packet header
a

Figure 3A

Figure 3B


a
328
Build a request packet into the write token.
330
Signal the write thread of the communication channel to send to packet.
332
Release the write token for other use
334
Error in sending the packet
Yes
No
336
Wait for the response packet
338
Transfer data in the response packet to the application's buffer.
340
Signal the read thread of the comm channel that the read token is no longer in use.
342
Destroy the response signal.
344
Return control to the application.

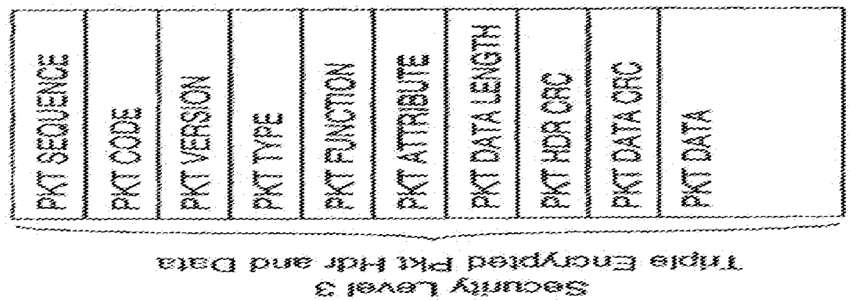


Figure 4C

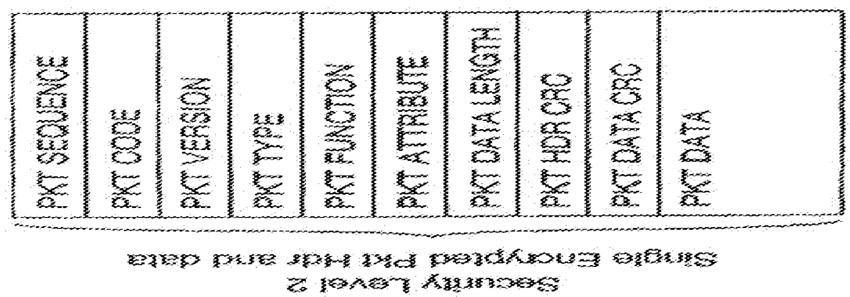


Figure 4B

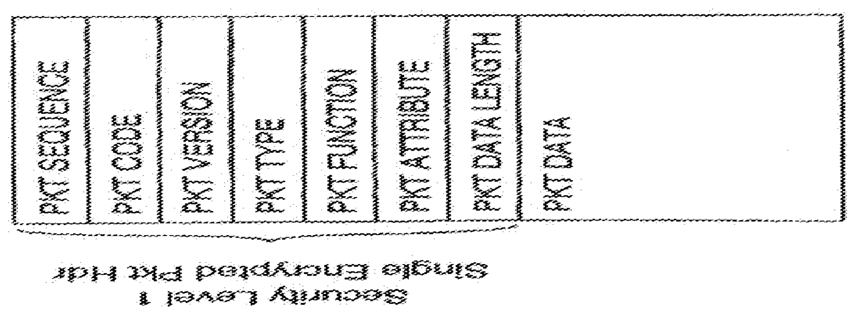


Figure 4A

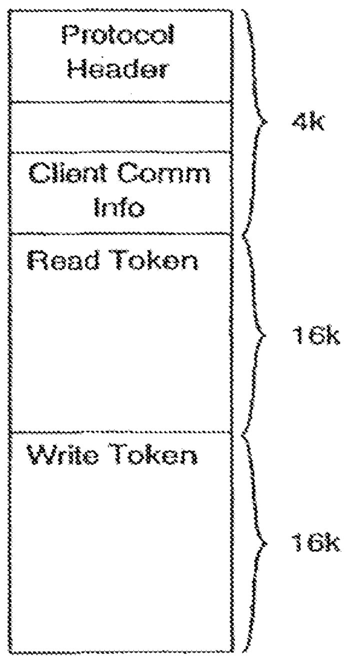


Figure 5A

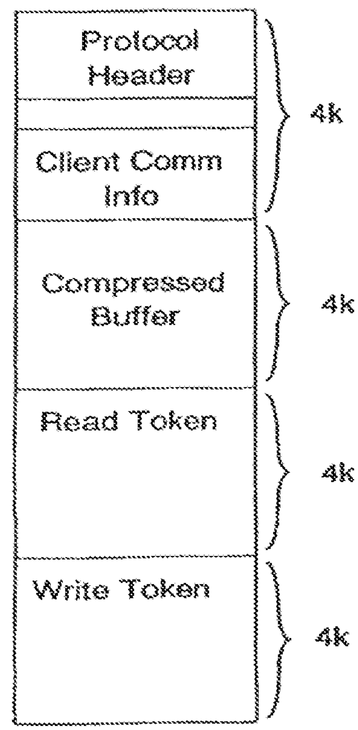


Figure 5B

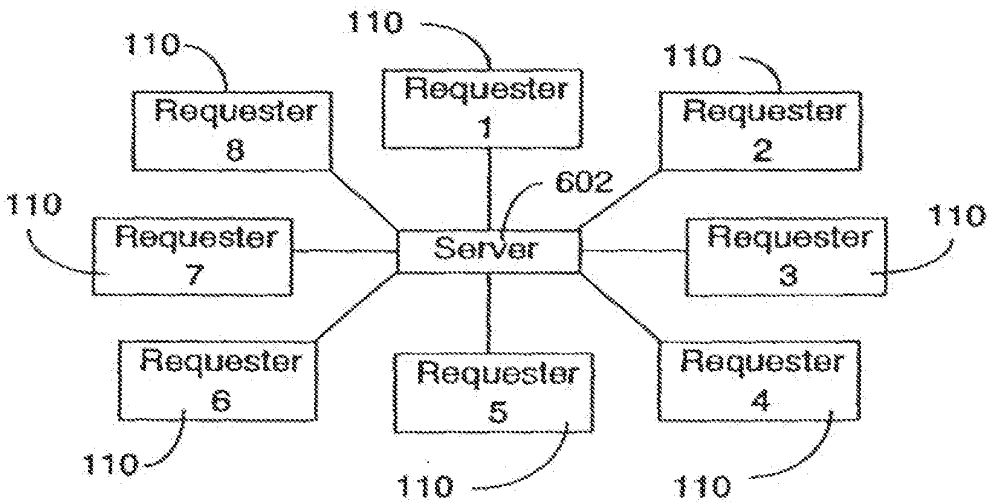


Figure 6

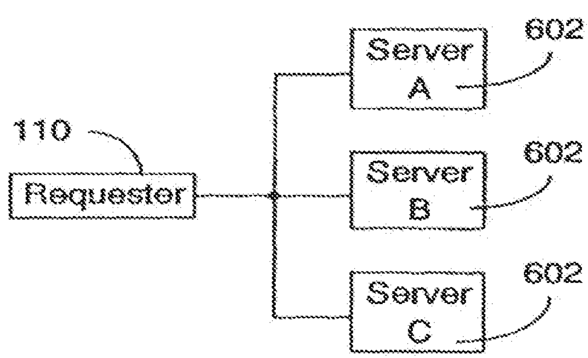


Figure 7

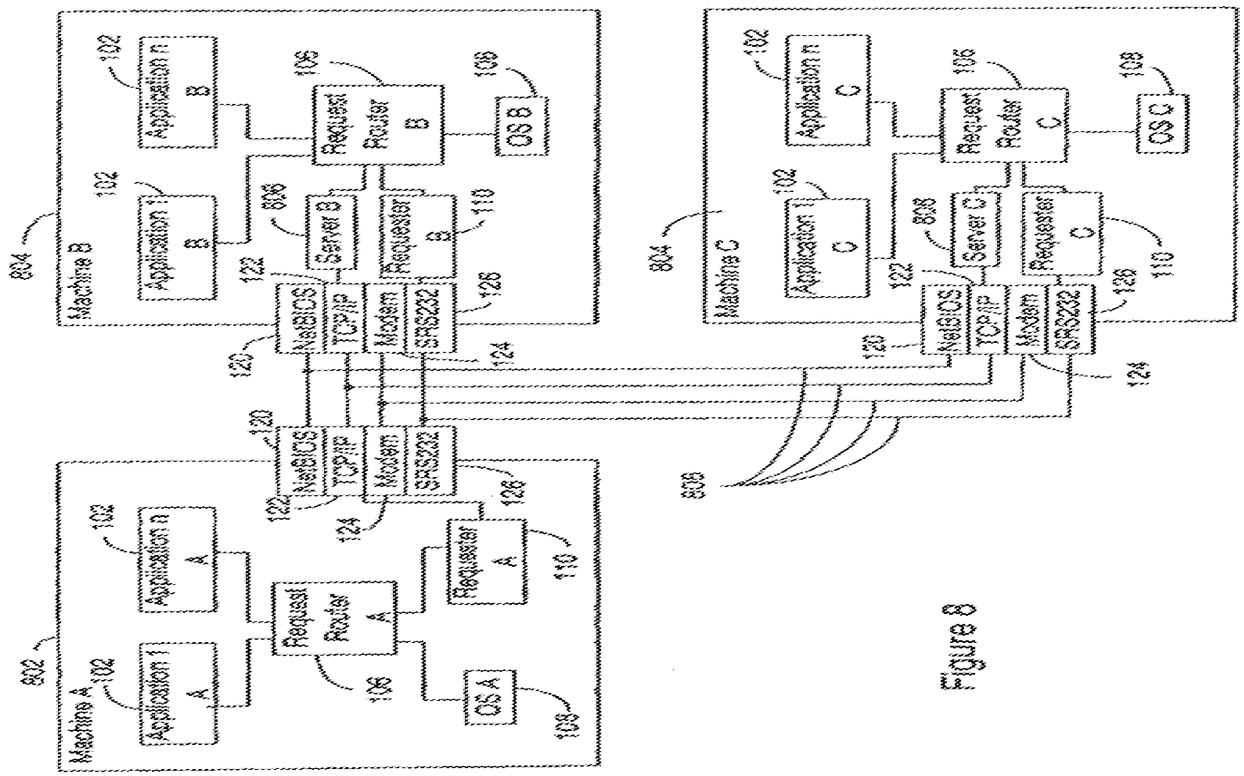

802
Machine A
102
Application 1
A
102
Application n
A
Request
Router
A
106
OS A
108
Requester
A
110
120
122
124
126
NetBIOS
TCP/IP
Modem
SRS232
804
Machine B
102
Application 1
B
102
Application n
B
806
Server B
Request
Router
B
106
Requester
B
110
OS B
108
804
Machine C
102
Application 1
C
102
Application n
C
808
Server C
Request
Router
C
106
Requester
C
110
OS C
108
808

Figure 8

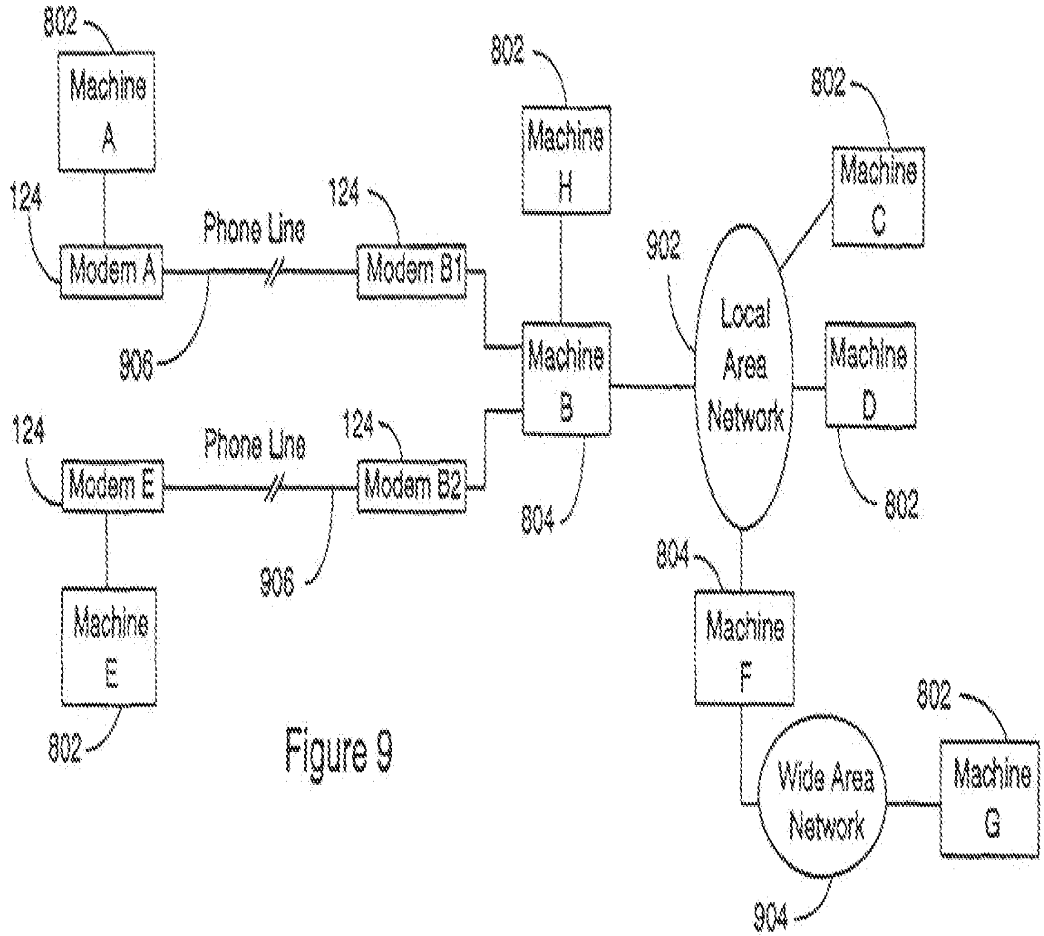

802
Machine A
124
Modem A
Phone Line
906
124
Modem B1
802
Machine H
Machine B
804
124
Modem E
Phone Line
906
124
Modem B2
Machine E
802
902
Local Area Network
802
Machine C
Machine D
802
804
Machine F
Wide Area Network
904
802
Machine G

Figure 9

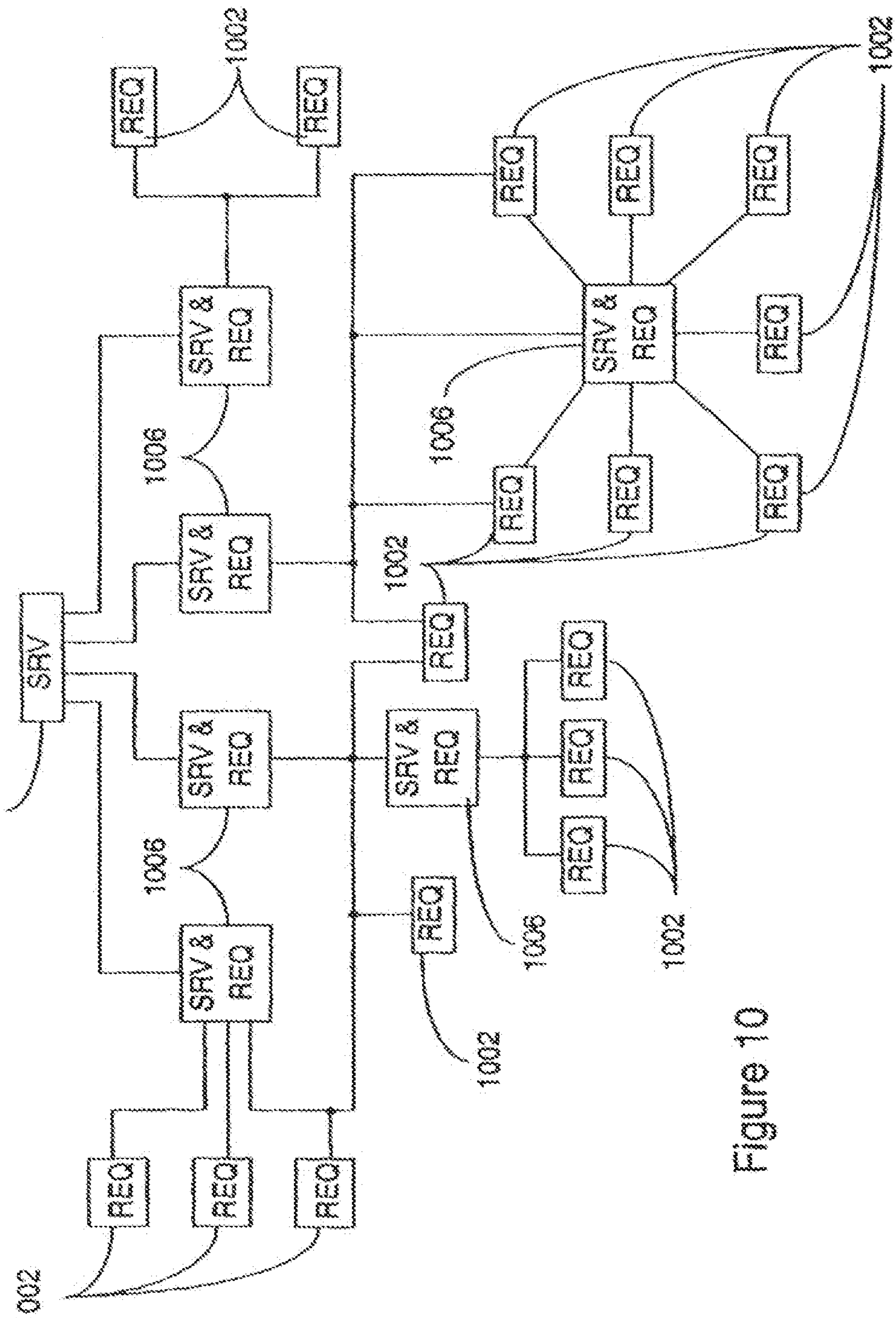


Figure 10

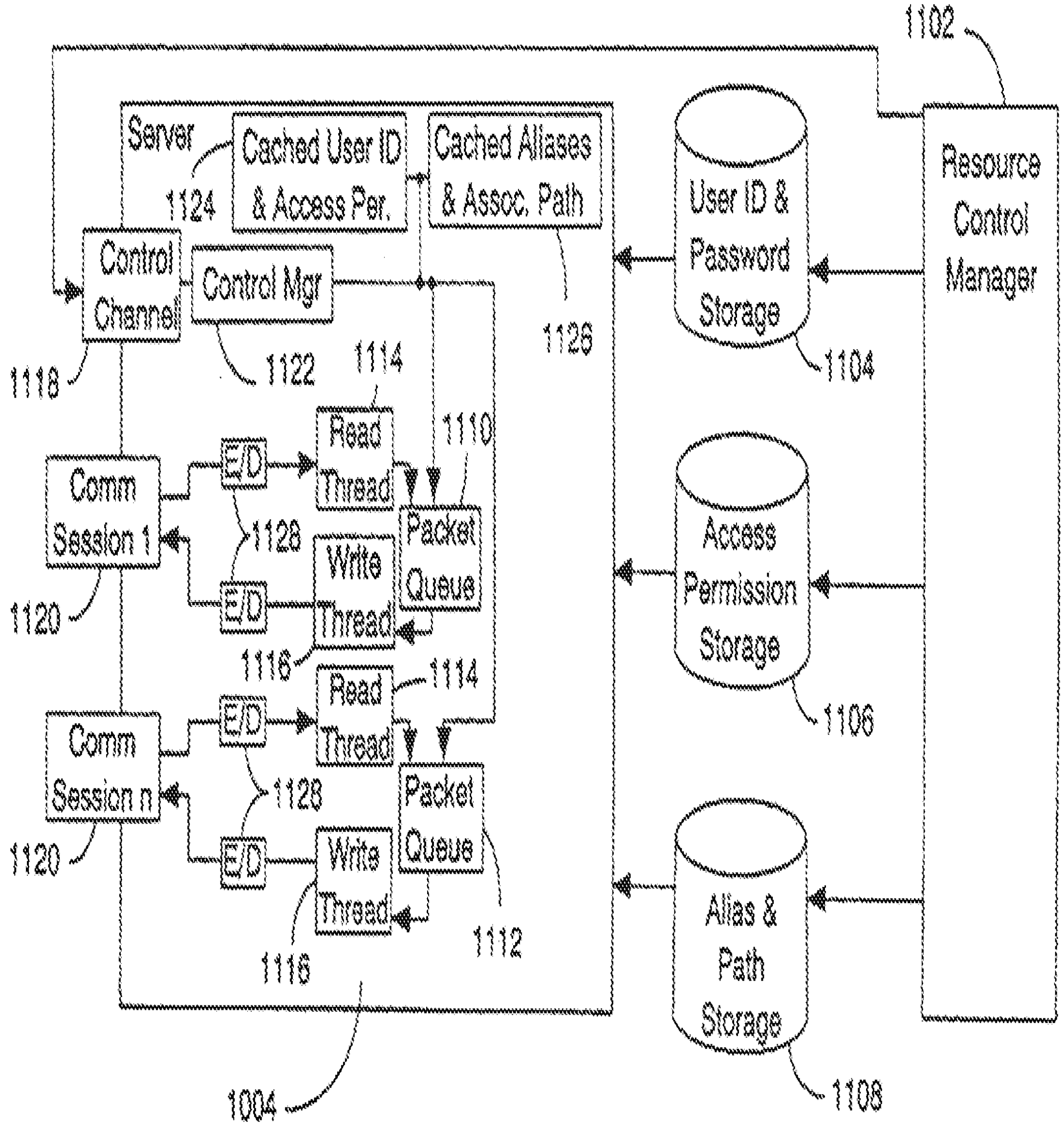

1102
Resource Control Manager
User ID & Password Storage
1104
Access Permission Storage
1106
Alias & Path Storage
1108
Server
Cached User ID & Access Per.
1124
Cached Aliases & Assoc. Path
1126
Control Channel
1118
Control Mgr
1122
Comm Session 1
1120
E/D
1128
Read Thread
1114
Write Thread
1116
Packet Queue
1110
Comm Session n
1120
E/D
1128
Read Thread
1114
Write Thread
1116
Packet Queue
1112
1004

Figure 11

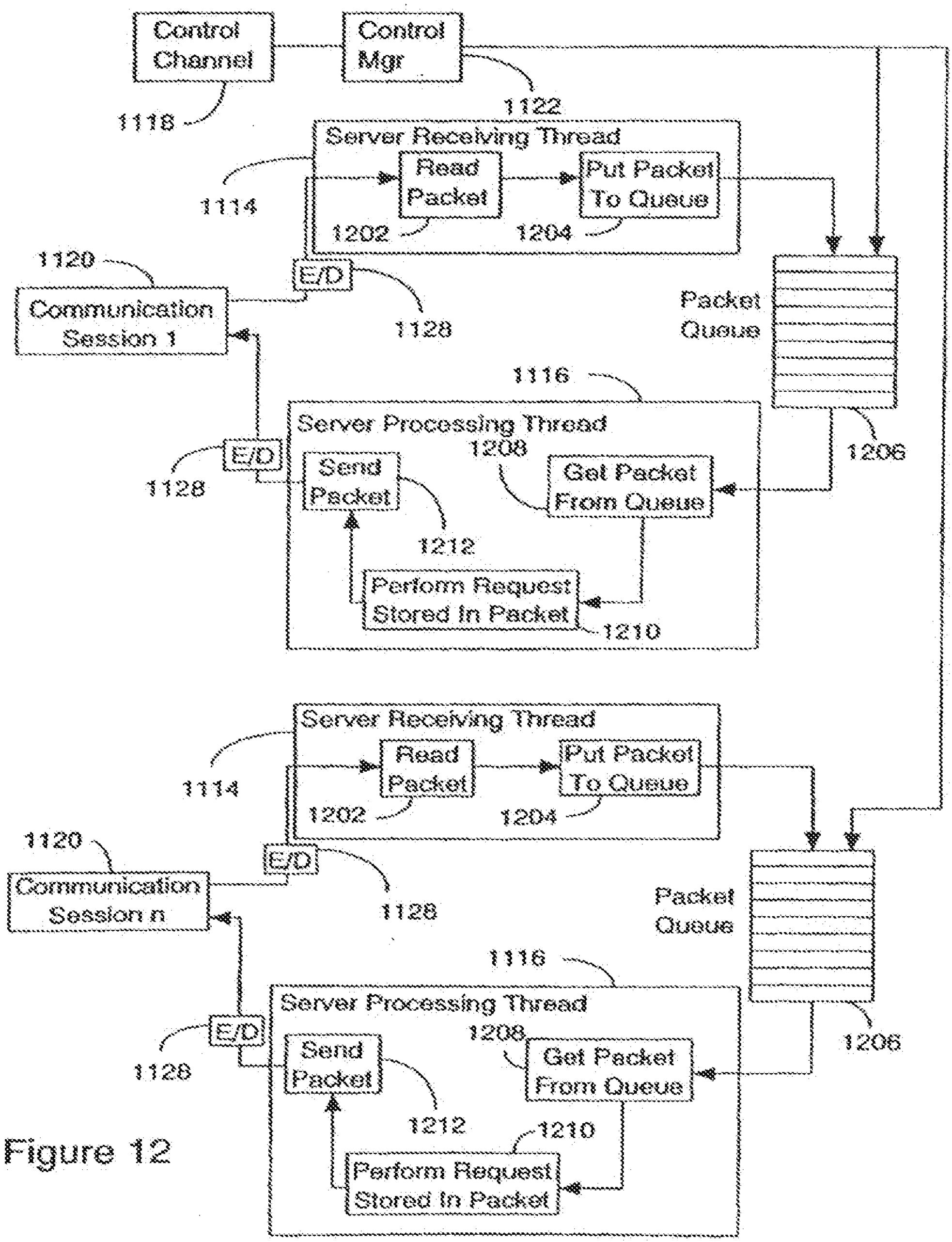

Control Channel
Control Mgr
1118
1122
Server Receiving Thread
Read Packet
Put Packet To Queue
1114
1202
1204
1120
E/D
Communication Session 1
1128
Packet Queue
1116
Server Processing Thread
1208
Send Packet
Get Packet From Queue
1206
1128
1212
Perform Request Stored In Packet
1210
Server Receiving Thread
Read Packet
Put Packet To Queue
1114
1202
1204
1120
E/D
Communication Session n
1128
Packet Queue
1116
Server Processing Thread
E/D
1208
Send Packet
Get Packet From Queue
1206
1128
1212
1210
Perform Request Stored In Packet

Figure 12

Figure 13A

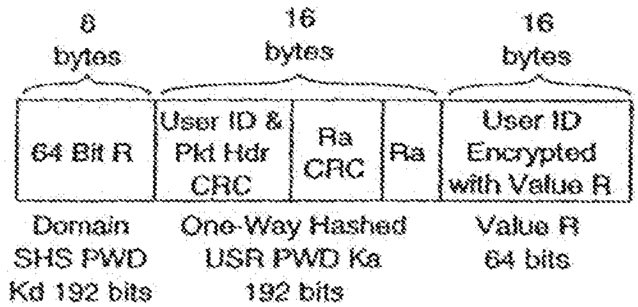


Figure 13B

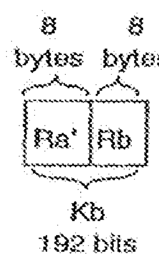


Figure 13C

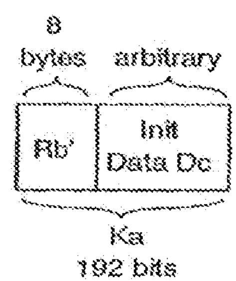


Figure 13D

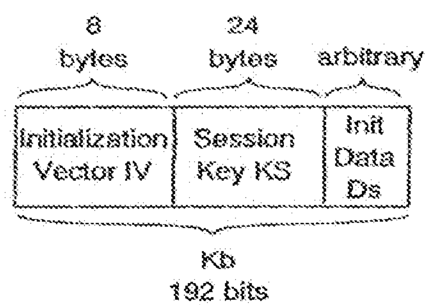
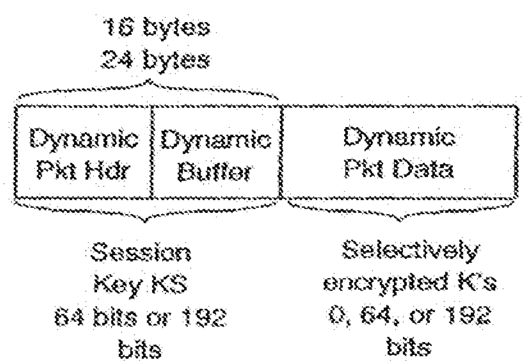


Figure 13E



NETWORK WITH SECURE COMMUNICATIONS SESSIONS

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates to computer network security. In particular, it relates to networks which use dynamic packet headers and multiple levels of packet encryption to transfer data to and from a remote server or to and from another node in the local network.

2. Background Art

The development of small independent systems such as personal computers has provided several benefits to users. By providing each user with their own processor and data storage, personal computers provide consistent performance and data security. A cost of these benefits is the inconvenience which results from the inability to easily access data by other members of an organization.

The use of mainframe systems, and the later development of alternative systems such as LANs (Local Area Networks) and servers reduces the inconvenience of making data available to all members of an organization, but results in unpredictable performance, and more importantly results in exposure of sensitive data to unauthorized parties. The transmission of data is commonly done via packet based systems which have user ID and password information in a header section. Interception of a packet with header information allows the interceptor to learn the user ID and password which will in turn allow future penetration of the user's system and unauthorized access to the user's data. It would be desirable to transmit user identification and password information in a manner which would be indecipherable to an unauthorized interceptor.

Data security is endangered not only by access by outside parties such as hackers, industrial spies, etc, but also to inadvertent disclosure of data to unauthorized members of the organization. For example, data exchange at certain levels of management may cause problems should the information be disclosed to the general employee population. Likewise, the transmission of personal information such as banking codes over networks has exposed individuals using online financial systems to the possibility of fraudulent access to their funds by third parties.

In addition to data security, the use of network systems such as LANs has created performance problems due to the queuing of requests from multiple locations and the unpredictable delays associated with queuing fluctuations. It would be advantageous if a system could provide not only data security, but also more consistent performance.

The prior art has failed to provide network systems which ensure that access to data is restricted to authorized parties while at the same time providing more consistent performance.

SUMMARY OF THE INVENTION

The present invention solves the foregoing problems by providing a system which uses three way password authentication, encrypting different portions of a logon packet with different keys based on the nature of the communications link. Nodes attached to a particular LAN can have one level of security for data transfer within the LAN while data transfers between LANs on a private network can have a second level of security and LANs connected via public networks can have a third level of security. The level of security can optionally be selected by the user. Data transfers between nodes of a network are kept in separate queues to reduce queue search times and enhance performance.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram showing the connection between applications and the requester in a local system.

FIG. 2 is the diagram of FIG. 1 with a more detailed view of the requester.

FIGS. 3A–B are a flow diagram illustrating data transfer between the application and requester of the preferred embodiment.

FIGS. 4A–C are diagrams of the memory layout of packet headers used in the preferred embodiment.

FIGS. 5A–B are diagrams showing the memory layout of entries in the packet queue. FIG. 5A is the memory layout used for TCP/IP and NetBIOS. FIG. 5B is the memory layout used by SMODEM or SRS232 communications systems.

FIG. 6 is a diagram of a multi-requester system with a single server.

FIG. 7 is a diagram illustrating a single requester attached to three servers.

FIG. 8 is a diagram showing a requester (machine A) interconnected with two servers (machines B–C).

FIG. 9 is a diagram illustrating multiple requesters connected to servers via local area networks (LANs) and wide area networks and public telephone networks.

FIG. 10 is a diagram illustrating multiple requesters connected to servers and server/requester systems.

FIG. 11 is a diagram illustrating the server used in the preferred embodiment.

FIG. 12 is a diagram illustrating the read/write threads and packet queues used by the server of FIG. 11.

FIGS. 13A–D are diagrams illustrating the packet headers used in the logon procedure of the preferred embodiment.

FIG. 13E are diagrams illustrating the packet headers used during data transfer in the preferred embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Prior to a detailed description of the figures, a general discussion of the operation of the preferred embodiment follows. A network can take a variety of forms. For example, it can be two personal computers communicating via modem; it can be a single LAN system within a particular facility; it can be a remote server or mainframe system with communications links to individual terminals or personal computers; it can be a network of LANs or other servers each communicating with one another or through one another; or it can be any of the foregoing systems which use not only dedicated communications lines, but also nondedicated communications (i.e. public networks such as the Internet) through a "firewall". The use of the term firewall herein refers to the requirement for increased levels of security to avoid the possibility of unauthorized data access by parties outside of the organization. Likewise, a machine in the network can act as a client or a server depending on the nature of the data transfer.

In the preferred embodiment, communication between a client and a server is as follows. The server waits for connection requests from clients on the network. The server can be started with one or more supported protocols to enable support of a variety of client types on the network.

For example, the server protocols can include, among others, NetBIOS, TCP/IP, SMODEM and SRS232. All of the foregoing protocols are well known in the art.

When a user on a client machine wishes to initiate a data transfer or other function, the client application activates a requester to access resources in the network. When the server receives a request from a client application, it activates a thread to process the request. A thread is an execution unit of an operating system. Operating systems used for this type of system are Microsoft Windows 95 (trademark of Microsoft Corporation), Microsoft Windows NT (trademark of Microsoft Corporation), IBM OS/2 (trademark of IBM Corporation). These systems may use multiple session protocols such as NetBIOS and TCP/IP or single session protocols such as SMODEM or SRS232.

In single session protocols such as SMODEM and SRS232, the same thread is used to process the request from a client since a serial port can act as a server or client, but cannot simultaneously act as a server and client. Multiple session protocols create a new thread, referred to as an original thread, and wait for a request from a client. When a request is received, the thread is referred to as a server processing thread which is used to process the client logon.

After the logon is successfully completed, the server processing thread creates a packet queue and a packet thread to receive incoming packets and place them in the packet queue. The server then waits for packets to arrive. On the client side, the client creates a session write thread to initiate contact with the server. In addition, the client creates a second thread which is referred to as the session read thread. This thread is used to receive packets sent from the server to the client.

To use resources on the network, users must first logon the server to prove their identity. A logon request is sent from the client's logon application to the requester on the client computer. Before logon data can be exchanged between the applications and the requester, a command manager is created by the requester to accept application requests. The command manager is responsible for housekeeping requests within the client computer.

In the preferred embodiment, the logon procedure uses a three way authentication to prevent the password from being transferred over the computer and also to allow both the client and the server to authenticate each other. In addition, the authentication procedure prevents unauthorized penetration of the system security by detecting the replaying of packets by third parties.

The three way authentication system encrypts the very first logon packet with different keys for each part of the packet as follows.

The first step takes place at the client computer as follows.

1—The client generates a 32 bit random number value which is concatenated to a predefined 32 bit constant to form a 64 bit value R.

2—The CRC signature C1 of the 64 bit value R and the user ID is calculated. This signature value allows detection of packet manipulation.

3—The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet.

4—The client generates a 192 bit key K from the server name to encrypt the 64 bit value R.

5—The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS) specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180).

6—The client generates a random number Ra, calculates its CRC signature C2, and encrypts them with the signature C1 using the key Ka. This signature is used to validate the key Ka by the server.

The second step in the process takes place at the server. When the server receives the first logon packet it decrypts the packet as follows.

1—The server generates a key K2 from its machine name and the SHS to decrypt the packet header for identification. If the packet header does not contain the predefined constant, the user is unauthorized. This occurs when an unauthorized user tries to access the server over the phone line but does not know the server name (since the phone number is a public record but the server name is private).

2—If the user is authorized, the server uses the decrypted 64 bit value R in the packet header as a key to decrypt the user ID.

3—The server then uses the user ID to search a database for an access record. If the access record cannot be found, the user has entered an invalid ID and the session is terminated. If the access record is found, the server verifies if the user is allowed access to network resources at this date and time.

4—If access date and time are verified, the server retrieves an associated one way hashed password Kb from an encrypted password file to decrypt the random number Ra and the CRC signatures. The password file is encrypted with a key Kk which is selected by the system administrator at installation.

5—The random numbers Ra and the CRC signatures are then decrypted. The server calculates the CRC signature of the packet header, the user ID and the random number Ra. If the calculated signatures match the decrypted signatures C1 and C2 stored in the packet, and if password Ka matches Kb, the server manipulates the client random number Ra with a predefined formula, generates a random number Rb, and encrypts both random numbers Ra and Rb with the password Kb before sending the first logon response packet to the client.

The third step in the process takes place at the client computer as follows.

1—The client decrypts the first logon response packet.

2—The client manipulates the random number Ra with the predefined formula and compares it with the one returned from the server. If the numbers match, the client knows that it is connected to the correct server, not a fraud server from which an eavesdropper has captured transmissions from the previous logon and is echoing packets back to the client computer.

3—The client manipulates random number Rb with another predefined formula and concatenates it with the client's initiating data (i.e., the client initial packet sequence number, the encryption and compression mode for the session, and the operating system platform ID) to form a second logon packet. The operating system platform ID is useful for selecting protocols and data formats when a particular client or server is communicating with systems that may have any one of a variety of operating system software programs running. The client would typically request encryption and compression mode for the session. However, the server may indicate that the particular modes requested are not available.

4—The client then encrypts the second logon packet and sends it to the server.

The fourth step in the process takes place at the server computer as follows.

1—The server decrypts the second logon packet.

2—The server manipulates the random number Rb with the same predefined formula used by the client and verifies if the random numbers are matched. If the random numbers match, then the server knows it is communicating with an authorized client and that the first logon packet was not a replayed packet.

3—The server saves the client initiating data, generates a session key Ks and an initialization vector IV. In the preferred embodiment, Ks and IV are generated using the formula specified in Appendix C of the ANSI X9.17 standard.

4—Ks and IV are sent to the client along with the server initiating data (i.e., the server initial packet sequence number, supported and/or approved encryption and compression modes for the session, and the server operating system platform ID).

The client and server initial packet sequence numbers are used to detect packet deletion and insertion for data exchanged after the logon procedure.

The fifth step in the process takes place at the client computer as follows.

1—The second logon response packet is decrypted by the client.

2—The client encrypts Ks and IV with its own key and saves them in memory for future communication with the server. The logon procedure completes here.

After the logon procedure is successfully completed, all packet headers are encrypted using the session key Ks and the IV. The packet headers are encrypted to prevent intruders from deleting, inserting, modifying, and/or replaying the packets which may have been captured while data was exchanged over communication lines.

For ease of illustration, the following symbols can be used to illustrate the logon process:

Where:

C=a client

S=a server

E=a symmetric cryptosystem such as DES

K=an encryption key generated from the server name

R=a 32 bit random number concatenated with a pre-defined constant

Ka=a 192 bit key one way hashed from the user ID and password

Ra=a 64 bit random value generated by C

f( )=a hash function such as CRC to calculate the signature

g( )=a hash function such as CRC to calculate the signatures

UID=user IDs

Kb=a 192 bit one way hashed key retrieved from a database

ha( )=a hash function to manipulate the random number Ra

Rb=a 64 bit random value generated by S

hb ( )=a hash function to manipulate the random number Rb

Dc=client initial data

IV=an initial chaining vector for encryption

Ks=a session encryption key

Ds=server initial data

R'a=ha(Ra)

R'b=hb(Rb)

The logon procedure may be listed as:

1. C to S: EK(R)+EKa(Ra,f(Ra,g(R,UID)))+EK(UID)

2. S to C: EKb(R'a,Rb)

3. C to S: EKa(R'b, Dc)

4. S to C: EKb(IV,Ks,Ds)

An important advantage of the authentication procedure used by the preferred embodiment is that both the client and the server verify each other as legitimate without sending the password. In addition, the use of a second set of logon packets which contain different encrypted random numbers precludes access by an unauthorized intruder who merely replays intercepted packets.

The heart of this authentication procedure is in the middle part of the logon packet, which contains the random number Ra and the CRC signatures. Since the CRC signature C2 of the random number Ra is encrypted and sent along with the logon packet, the server can authenticate the user right on the first logon packet. The manipulation of the random numbers Ra and Rb in the challenge-response fashion is to help the server defeat the replaying of the logon packet and to allow the client to authenticate the server and to defeat packet replaying as well.

The 32-bit random number in the packet header is used to make the packet header and the user ID look different for every logon packet. The one-way hashed server name is used as a key to quickly detect invalid logon packets before searching the database. This case may occur frequently when the ZMODEM protocol is activated to wait for data transferred over a telephone line (i.e., a wrong number is dialed by accident or a call generated by a manual or automated telemarketing company is being received).

In addition, the server name is isolated from the user ID and password when creating a one-way hashed password to allow the portability of the database. For example, when a business grows, another server may be needed at another location and the database can be easily transferred to the new server. Of course, it would be less time-consuming to delete unauthorized users from the database than to add authorized users to the new one. To better protect the valuable information in the database, a password is required before access to the database is granted. More important, the database can be shared among servers. For example, a server Sb can receive the first logon packet and forward the user ID to a database server Sc within a private network for verification. If an access record is found and the user can access the server Sb at this date and time, the database server Sc returns the encrypted one-way hashed password Kb to the server Sb. The server Sb then continues the challenge-response as if the password Kb is returned from a local database. Note that the database server Sc encrypts the one-way hashed password Kb with the session key defined for communication between the server Sb and Sc before sending it across the private network.

In comparison to prior art systems, the design of this invention provides the server a better opportunity to resynchronize itself if the first logon packet is invalid since the receiver of the authenticating packet is in control of what is next, not the sender. On the other hand, in the prior art the sender is in control of what is next. For example, the sender generates a public key, encrypts it with a shared secret key and sends it to the receiver. If the secret key is invalid, the receiver cannot detect it. Thus, a certain number of packets must be received before the receiver can resynchronize or the receiver might have to use a timeout to resynchronize itself.

Finally, the logon protocol of the preferred embodiment is more suitable for a client/server distributed environment, because this logon protocol allows both client and server to authenticate each other without sending the user password across the communication media and prevent intruders from deleting, inserting, modifying, or replaying the logon packets. In addition, if the logon procedure fails at any point, the server releases all resources and destroys the connection without sending the response packet at that point, i.e., if the user enters a wrong server name in the very first logon packet, nothing is sent out from the server to prevent the user, a potential intruder, from knowing anything about the server. Note that this mutual authentication technique requires the client machine to have a local CPU so that the password will not be transmitted over the network before being encrypted.

The client can now perform a mounting procedure to link a network resource on the server to a virtual disk or it can identify a network resource with the following format \\servername\netname:protocol. The format allows the client to communicate with a network domain using any supported protocols. Further, this protocol can be different from the protocol used to perform the logon procedure. That is, the logon communication protocol can be different from the mounting communication protocol. Also, different virtual disks can be mounted with different protocols to different network domains. This method allows communication between a client and network domains, between a network domain and other network domains using multiple communication protocols simultaneously.

Referring to FIGS. 1 and 2, these figures illustrate the interconnection between a client and a server. FIG. 2 is a more detailed view of the system of FIG. 1.

To perform a file transfer operation, an application **102** calls a request router **106**. The request router first verifies if the application **102** requests a local or remote resource. This verification is performed using a local mounting table **104** which the request router **106** obtains from the requester **110** when the application **102** is first started.

If the resource is local, the request router **106** calls a local system function call to perform the request and returns the control to the application **102**. However, if the resource is remote, the request router **106** first searches its local list to see if the needed communication handle is already stored in the list. This communication handle contains information of the read **204** and write **208** tokens (shown in FIG. 2) and their associated resources. If the communication handle is not found in the local list, the request router **106** sends a message to the requester **110** over the request channel **112** to obtain the handle. Once the handle is obtained, the request router **106** creates a response signal, i.e., a return address, requests the ownership of the write token **208**, stores the response signal into the packet header, builds a packet based on the application's **102** request into the write token **208**, and signals the session write thread **206** of the communication channel **114** that there is a packet to send.

If the application data is larger than the packet capacity, the request router **106** can send multiple packets in a series at this point. After the packet is sent to the server, the request router releases the write token for use by another thread in the same process or a different process. If the packet was sent to the server successfully, the request router **106** waits for the corresponding response packets, i.e., a packet can cause multiple response packets returned from the server.

When a response packet arrives, the session read thread uses the response signal to tell the corresponding request router that its response packet has come and is available in the read token. At that time, the read token is accessed exclusively by the designated request router. The router then transfers data in the response packet directly to the application's buffers and signals the session read thread **202** of the communication channel **114** that the read token **206** is no longer in use so that the session read thread **202** can re-use the read token **206** for other incoming packets. Finally, after all response packets of a request packet have arrived, the request router **106** destroys the response signal and returns control to the application **102**. The final response packet is determined by a bit in the packet attribute.

The request router **106** sends a message to the command manager of the requester **110** to request the communication handle containing information of the read **204** and write **208** tokens and their associated resources. If the handle already exists, it is passed to the request router **106** immediately after the requester **110** increments the access count of the handle. However, if the handle does not exist at that time, the requester **110** will load the appropriate communication library, allocate the tokens **204**, **208** and their associated resources, create a communication channel consisting of a session write thread **206** to perform auto-logon, create a session read thread **204** for the communication channel **114** if auto-logon is successful, and increment the access count of the handle before passing it to the request router **106**.

After receiving the handle, the request router **106** saves the handle for use during the entire lifetime of the application. When the application **102** terminates, the request router **106** will signal the requester **110** of the event so that it can decrement the access count of the handle. When the access count is zero for a certain period of time, the session manager of the requester **110** will drop the communication session, release the tokens **204**, **208** and their associated resources, and unload the communication library. Thus, this method allows resources to be allocated upon demand and released when no longer in use. Furthermore, the request router **106** can translate and format data in the application timeslices while the requester **110** is communicating with communication devices **120**, **122**, **124**, **126** to better use the CPU time.

The request router **106** can also perform any preparation necessary to transfer the application **102** request to the requester **110** before requesting the ownership of the write token **208** to reduce the time it takes to access the write token **208**. In addition, the request router **106** remembers resources for one application **102** at a time. Thus, it reduces the time to search for the needed information. With this method of sending and receiving packets, data can be exchanged asynchronously between a client and a server with minimum resources in a minimum time. In addition, request packets can be accumulated on the server for processing while the previous response packet is processed by the communication devices **120**, **122**, **124**, **126** or traveling over the network.

Message channel **128** and message manager **130** are used to control system messages transmitted in the system. Current mounting table **134** and global mounting table **132** are used to identify usage of system resources. The session control manager is used to control each session between a client and a server.

FIG. 3A and B is a flowchart which illustrates the transfer of information in a session after the logon procedure has completed. When a resource request **302** is made, the system **304** first tests to see if it is for a local resource **304**. If so, a local function is called **312** and control is returned **310** to the application. If it is not a local resource, the system creates a response signal **306**. If the response signal **306** cannot be created, control is returned to the application. If it is, then the local list is searched **314** for the communication handle. If the communication handle is not found **316**, a communication handle is obtained **318** from the requester and then ownership if the write token is requested **320**. However, if the communication handle is found **316**, then ownership if the write token is immediately requested **320**.

If no error occurs when the request for ownership of the write token is made **322**, then the response signal is stored in the packet header 326, a request packet is built into the write token 328, the write thread sends the packet, and the write token is released 332. If an error is detected when the packet is sent, the response signal is destroyed 342 and control is returned 344 to the application. If no errors occur during packet transmission 344, then the system waits 336 for the response packet, the data in the response packet is transferred 338 into the application's buffer, the read token is released 340, the response signal is destroyed 342 and control is returned 344 to the application.

FIGS. 4A–C illustrate the memory layout of the packets used in the preferred embodiment. FIG. 4A illustrates a packet as encrypted by security level 1. In security level 1, the packet header is encrypted using single DES encoding. This level of security incurs the least amount of overhead and is preferably used in more secure environments such as LANs.

FIG. 4B illustrates a packet as encrypted by security level 2. In security level 2, the packet header and data are encrypted using single DES encoding. This level of security incurs slightly increased overhead as compared to security level 1, but provides an increased level of security for less secure environments such as wide area networks.

FIG. 4C illustrates a packet as encrypted by security level 3. In security level 3, the packet header and the data are encrypted using triple DES encoding. This level of security incurs the most overhead as compared to security levels 1 and 2, but provides the highest level of security for insecure environments such as public telephone networks.

To protect data exchanged over communication sessions, the preferred embodiment provides two different encryption schemes available to the user at logon. The first scheme is the US Department of Defense Data Encryption Standard (DES) and the second scheme is the triple-DES specified in the ANSI X9.17 and ISO 8732 standards but with three different keys. In addition, the preferred embodiment applies the Cipher Block Chaining mode specified in the FIPS PUB 81 to better protect the data. Once an encryption scheme is selected, data exchanged over all sessions connected to a network domain are encrypted regardless of the communication protocols being used by the sessions. The price to paid for the encryption is minimum anyway since the preferred embodiment encrypts 500,000 bytes per second when running on a Pentium 66 MHz processor. The operating system used can be any suitable personal computer operating system such a Microsoft (TM) Windows 95 (TM), IBM (TM) OS/2 Warp (TM), Unix, etc. If the server is a large system, any one of a number of suitable mainframe operating system software may be used.

In addition to the above encryption schemes, the preferred embodiment employs a dynamic packet header technique to provide extra securities based on the security level selected by the user at logon. If a security level 2 is selected, the packet header and data are encrypted with DES and the packet header is changed to 24 bytes to carry the CRC signatures of the packet header and data for authentication. However, if a security level 3 is selected, the packet header and data are encrypted with triple-DES using three different keys. Finally, if security level 1 is selected, the packet header remains at 16 bytes and no signature is verified for a better performance but the packet header is encrypted with DES to provide security against other threads. Thus, thanks to the dynamic packet header technique, a user can setup different types of firewalls wherever he needs them. For instance, the user can connect to his office from his home using security level 2 and setup his office machine to connect to another server within his organization using a lower security level to gain a better performance.

In order to provide better security, the preferred embodiment allows the user to select if the data should stay in its encrypted form so that only authorized personnel can view the data. This is important for sensitive business data, personnel data, etc. Of course, the key to decrypt the data must be agreed to ahead of time or exchanged over some secured channels to protect the secrecy of the key.

Of course, those skilled in the art will recognize that the user could also have the capability of instructing the system that no encryption will be used. In this case, no encryption would represent a fourth security level (security level 0). Security level 1–3 having been discussed in regard to FIG. 4.

FIGS. 5A–B illustrate the packet queue structure used in the preferred embodiment. FIG. 5A illustrates the TCP/IP and NetBIOS communications structure and FIG. 5B illustrates the SMODEM and SRS232 communications structure. The compressed buffer is a work buffer used to compress data prior to transmission through SMODEM or SRS232 communication lines. A packet header is placed at the beginning of the read token and at the beginning of the write token. In the preferred embodiment, the read and write tokens are stored in shared memory.

FIG. 6 illustrates a configuration in which multiple requesters 110 communicate with a single server 602.

FIG. 7 illustrates a configuration in which a single requester 110 communicates with multiple servers 602.

FIG. 8 illustrates a configuration in which a system 802 and multiple servers 804 communicate with one another.

FIG. 9 illustrates a configuration in which multiple systems 802 and multiple servers 804 communicate with one another via modems 124 over phone lines 906 and also over LANs 902 and wide area networks 904. This figure illustrates the ability of the system to interface with multiple communications protocols.

FIG. 10 illustrates a configuration in which multiple requester systems 1002, multiple server systems 1004, and multiple server/requester systems 1006 communicate with one another. The configuration in this figure is similar to that shown in FIG. 9.

FIGS. 11 and 12 illustrate a configuration in a server 1004 which includes communication sessions 1120 to communicate with requesters, encrypter/decrypter 1128, read threads 1114, write threads 1116, packet queues 1110, 1112, a resource control manager 1102 to control user ID, access permission and alias and path storage 1104, 1106, 1108. The cached user ID and access permission 1124 and the cached alias and associated path 1126 caches are used to store data from the access permission storage 1106 and the alias and path storage disks 1108 for improved system performance.

To protect resources on the network domains, an access control list (ACL) is used for each network domain in access permission storage 1106. The ACLs are managed by network administrators to define to which resources a user can access and what kind of accesses the user has to each resource. The system provides a sophisticated ACL so that a user cannot view or access any resources other than those assigned. The following access permissions are used by our ACLs:

READ_FILE
WRITE_FILE
CREATE_FILE
DELETE_FILE
EXECUTE_FILE
CHANGE_ATTRIBUTE
ACCESS_SUBDIR
CREATE_SUBDIR
REMOVE_SUBDIR

For example, if the user is not permitted access to any subdirectories from a network resource, the user will not see any subdirectory at all when viewing the network resource. If for some reasons the user knows a particular subdirectory exists under the network resource, he cannot access it anyway. The management of network resources and user access permissions is provided with a user-friendly Graphical User Interface application. Together with the logon procedure, ACLs provide effective protections to the resources on the network domains.

FIG. 12 is a more detailed view of the server 1004 of FIG. 11. A control manager 1122 within the server 1004 is responsible for communication between the server 1004 and other applications on the server 1004 machine. Thus, the server 1004 can be informed if a database has been changed by a resource control application. The server 1004 can also accept a message from another application 102 to send to all or selected clients over active sessions. If an electronic mail system should be needed, the server 1004 can save the message and wait until a client is logged on to send the message over the session. To support these features, the control manager 1122 posts message or e-mail packets to the incoming packet queues 1206 of the sessions 1120. When the server processing threads 1114, 1116 of the sessions 1120 retrieves the packets from the queue 1206, it will process the packets based on the packet types defined in the packet headers.

FIG. 13A–D illustrates the packet headers used in the logon procedure. A session key KS and an initialization vector IV are defined for a communication session between a client and a server 1004 when security level 1 or higher is desired (in security level 0, no encryption is used).

FIG. 13E illustrates a normal packet such as those used during data transfer. When an e-mail or message packet is sent, the preferred embodiment uses security level 2 by default to protect the messages. In security level 2, both packet header and data are encrypted using single DES encryption.

The requester also has the capability to signal request routers 106 of all applications 102 when a communication session is terminated abnormally whether the request routers 106 are sending request packets or waiting on response packets. In order to perform this feature, the response signals (i.e., the return addresses stored in the request packets) are saved in response-signal queues by the session write thread 1116. Each communication session has a response-signal queue 1206 to reduce the search time. When the response packets are successfully delivered, their corresponding response signals are removed from the queue by the session read threads 1114 of the corresponding communication channels. If an application 102 terminates before its response packets arrive, the response packets are discarded and the response signals are also removed from the queue after all chaining response packets have arrived.

In addition, the read thread of the client session also recognizes different types of packets to determine whether it should route the received packets to the application's request router or to a message manager within the requester. The message manager of the requester is responsible for message and e-mail packets sent from the connected servers. This feature is important because it allows the server to initiate the sending of packets while a session is active. As an example, a hot-link can be defined so that a server can inform the connected clients if a database should be changed or a server administrator can send a message to all or selected clients telling them if a server should be out of service shortly, etc. In a more advanced application, an electronic-mail server application can be written so that the message packets are saved on the server until a client is logged on. At that time, the server will send the saved messages to the connected client.

In the prior art, the requester is the one that translates and formats requests from the applications; thus, it cannot perform preparation ahead of time. In addition, information accumulating in one place could increase the search time. The prior art requires its intrinsics modules in both the application and the requester which may require more resources to be allocated and more machine instructions to be executed. Furthermore, the prior art does not have the capability to accumulate multiple request packets from a requester so that the server can process the next packet request while the previous response packet is traveling back to the requester on the network or being processed by communication devices in their own memory buffers.

In contrast to the prior art, the preferred embodiment contains the formatting and translating code in just one place, the request router 106. Our requester only encrypts packet headers and packet data if necessary and then calls the transport functions to send the packets to the server. In addition, requester 110 is also responsible for saving logon and mounting information, managing the communication sessions, and delivering response packets received from multiple network domains to multiple request routers while sending request packets to the multiple network domains. Requester 110 does not need to know the format of the response data, and can deliver the response packets immediately upon receiving them. The request routers 106 can then format or translate the response data in the applications timeslices while the requester 110 is waiting for other incoming response packets or reading data from the communication devices 120, 122, 124, 126. Thus, the preferred embodiment achieves better performance than the prior art.

The prior art also requires the intrinsic modules to translate and format the application data from a program stack segment to a parameter block before sending it to its requester where the data is once again formatted or copied into a data communication buffer. In contrast, the request routers 106 in the preferred embodiment format the application data only once and store the formatted data into the write token which will be used by the requester and the communication subsystem to send the request packets to the server. When the response packets arrive, the requester 110 uses the response signals to tell the corresponding request routers that their response packets have arrived. At that time, the request routers 106 transfer response data directly from the read tokens into the application buffers. Thus, the preferred embodiment eliminates the overhead of copying data between memory buffers.

Furthermore, the prior art does not have the dynamic packet header feature to support packet authentication on demand. Neither does its server authenticate the requester to prevent replaying of packets by intruders. The prior art also requires two different programs running on the server to wait for incoming data from different communication protocols. The preferred embodiment only requires the server to be started once for multiple communication protocols.

In general, a session on the server 1004 will support multiple applications on the requester; thus, a server 1004 must somehow remember the resources allocated for the client applications so that these resources can be released whether the client applications terminate abnormally or the communication sessions are destroyed abnormally. Our server supports this feature in each session thread. Since the allocated resources are isolatedly remembered for different requesters, the search time is minimum every time they are added or removed from the memorized list. In addition, security audit can be turned on and off by the network resource manager running on the server over the control channel of the server. The network resource manager can toggle the security audit for users or groups whose IDs are supplied in the auditing request packet, or resources whose names are stored in the auditing request packet. The audit can also be logged based on successful, failed, or both transactions.

In the prior art, the application is the one which determines if a session should be started on the host computer. The application then makes a function call to connect to the host computer and another function call to start a host server process. In the preferred embodiment, the session manager of the requester determines if a connection should be established to couple the client computer to the server computer. Once the connection is established, the server automatically creates a server processing thread to process the client request packets received over the connection. After the connection is established, the session manager also performs the auto-logon itself, not the application. The session can then be shared by all the applications on the client machine.

Thus, the session creation and logon are transparent to the applications. If the logon is successful, the server creates a server receiving thread to receive and accumulate request packets in a packet queue so that they will be processed by the server processing thread. When a session disconnect request packet is received, the server receiving and processing threads terminate themselves. However, if the communication session is destroyed abnormally, the server receiving thread simulates a disconnect request packet and appends it to the packet queue to signal the server processing thread to terminate. The server receiving thread then terminates itself.

Note that in the very first logon manually performed by the user, the operation is slightly different than the auto-logon mentioned in the above paragraph. The requester first receives a logon request from the logon application, it establishes the session itself and then performs the logon. This is so done by the command manager of the requester, not by the session manager.

Since request packets are accumulated in the packet queue in the preferred embodiment, the request packets may not be processed immediately upon arrival. In contrast, the prior art must process the request packets immediately to return the status or data to the requester. This may indicate that other applications on the client computer must wait until the return packet has arrived and processed before they can send their requests to the same host computer.

The prior art requires an application to send a function call to the host computer to established a communication session. Our system establishes a communication session by the requester when it receives a logon request from the logon program or a request router asking for the communication handle. In addition, our server has the capability to reformat and retranslate the request packets in its own request router before forwarding them to the requester located on the server when the network resources do not reside on the server. That is, multiple servers can be connected together as shown in FIGS. 7-10 to expand the amount of network resources available to requesters. Note that this feature requires the intermediate servers' administrator(s) to manually logon the designated servers since the logon passwords are not stored on the intermediate servers. Users on requesters can perform this logon remotely if their access permissions in the ACLs of the intermediate servers indicate that they can execute programs on the intermediate servers. However, caution must be taken and security level 3 is advised when using this feature since logon user IDs and passwords must be sent along with the executing request packets.

As shown earlier, the very first logon packet is encrypted with three different keys for different parts of the packet. The header of the logon packet is encrypted with a key generated from the server name. This is design to detect outside intruders early in the verification process. For intruders working inside an organization, the server name may be known. Then it comes the middle part of the logon packet which contains the 64-bit random number and the CRC values. These are the heart of the verification since it is encrypted with the key generated from the user ID and the secret password. This scheme allows the server to detect the intruding logon right on the very first packet. The challenge-response process that following the logon packet is to defeat re-played packets.

The encryption system used in the preferred embodiment has several other advantages, as follows. The long term key is derived from a user ID and a secret password. It has 192 bits and is used in a triple-DES encryption enhanced with CBC. The short term key is generated with the X9.17 key generation formula and changed every time a session is established between two nodes on the network. Thus, the encryption occurs at the application layer which exposes the source and destination addresses of the packets when used with TCP/IP and NetBIOS protocols but the intruders must deal with different keys whose lengths are either 64 or 192 bits for different pair of nodes on the network. In addition, the short term key is encrypted and only sent once when the communication session between two nodes is established, not in every packet; thus, it reduces the traffic between two nodes.

Furthermore, the prior art only protects data between site-firewalls, not between nodes. In many cases, data must be protected between nodes within an organization. For instance, high-rank management officers within a private network may want to exchange restricted confidential information without leaks to their employees.

Encryption at the application layer also reduces the cost of replacing the existing network layer and can be done on demand when protection to data is needed. Different security firewalls can easily be established between any pair of nodes with a single click of the fingertip.

Finally, the communication subsystem of the preferred embodiment is a foundation for multiple applications when their use are in demand. With just one communication session between a client and a server, packet sending can be initiated by either party to conduct file transfers, broadcast messages, or e-mail messages. In addition to minimum resources and maximum performance, security is also provided to protect the secret of the data.

While the invention has been described with respect to a preferred embodiment thereof, it will be understood by those skilled in the art that various changes in detail may be made therein without departing from the spirit, scope, and teaching of the invention. For example, the size of encryption keys can be changed, algorithms used to generate the encryption keys can be changed, the device can be implemented in hardware or software, etc. Accordingly, the invention herein disclosed is to be limited only as specified in the following claims.

I claim:

1. A bi-directional security system for a network, comprising:

at least one client, the client futher comprising:

client communication means to communicate with at least one server;

packet reception means to receive transmitted packet data from the server;

means to generate and transmit a first packet to the server, at least a portion of the first packet having a first packet header containing client identifying information;

means to encrypt at least a portion of the client identifying information in the first packet header prior to transmission;

means to decrypt at least a portion of the client authenticating information in a second packet header and to determine if the second packet is from the server, the client further having means to terminate the communication if the second packet is from an invalid server;

means to generate and transmit a third packet to the server, at least a portion the third packet having a third packet header containing session information; and

means to encrypt at least a portion of the session information in the third packet header prior to transmission; and

the server further comprising:

server communication means to communicate with the client;

packet reception means to receive transmitted packet data from the client;

means to decrypt at least a portion of the client identifying information in the first packet header and to determine if the first packet is from a valid client, the server further having means to terminate the communication if the first packet is from an invalid client;

means to generate and transmit a second packet to the client in response to the first packet, at least a portion the second packet having the second packet header containing client authenticating information;

means to encrypt at least a portion of the client authenticating information in the second packet header prior to transmission; and

means to decrypt at least a portion of the session information in the third packet header;

whereby, the client and the server each verify the validity of the other by transmitting encrypted identifying information to one another.

2. A security system, as in claim 1, further comprising:

means in the server to generate and transmit a fourth packet to the client in response to the third packet, the fourth packet having a packet header containing session information; and

means to encrypt at least a portion of the session information in the fourth packet header prior to transmission.

3. A security system, as in claim 2, wherein:

the client has a userid;

the client has a password;

the first packet is encrypted by:

concatenating a random number to a predetermined bit constant to form a value R;

a CRC signature C1 is generated from the value R and the userid;

the value R is used as a DES key to encrypt the userid;

the server name is used to generate a key K to encrypt the value R;

the key Ka is generated by a one way hash function from the userid and password; and

a random number Ra and its CRC signature C2 is generated, Ra and C2 are encrypted using key Ka.

4. A security system, as in claim 3, wherein:

the server further comprises an encrypted client password file;

the second packet is encrypted by:

a key K2 is generated from the server name and a one way hash function to decrypt the packet header of the first packet;

the userid is decrypted using the decrypted value R from the packet header;

the decrypted userid is used to access an authorization table to determine if the first packet is valid;

the userid is used to extract a one way hashed password Kb from the encrypted client password file, the password Kb is then used to decrypt values Ra, C1 and C2;

the value Ra is manipulated via a predetermined formula to produce a random number R'a;

a random number Rb is generated by the server; and

R'a and Rb are encrypted with password Kb, inserted into the packet header of the second packet and transmitted to the client.

5. A bidirectional security system for a network, comprising:

at least one client, the client further comprising:

means to encrypt a first logon packet;

means to transmit the first logon packet to the server;

means to decrypt the second logon packet;

means to encrypt a third logon packet with session information;

a server, further comprising:

means to decrypt the first logon packet;

means to encrypt a second logon packet with client authenticating information;

means to transmit the second logon packet to the client;

means to decrypt the third logon packet; and

a communication channel capable transmitting packets between the client machine and the server;

whereby the client and server can establish secure communications by bi-directionally transmitting encrypted data.

6. A security system, as in claim 5, further comprising:

means to encrypt packet data in least two security levels, the first security level having a first packet encryption scheme and the second security level having a second packet encryption scheme;

whereby the security system can selectably encrypt packet data with at least two packet encryption schemes.

7. A security system, as in claim 6, further comprising:

means to encrypt packet data at least three security levels, the third security level having a third packet encryption scheme;

whereby the security system can selectably encrypt packet data with at least three packet encryption schemes.

8. A security system, as in claim 7, wherein the first packet encryption scheme is a single DES encryption.

9. A security system, as in claim 8, wherein the second packet encryption scheme is a triple DES encryption.

10. A security system, as in claim 9, wherein:

the first packet encryption scheme encrypts the packet header information; and

the second packet encryption scheme encrypts the packet header information;

the third packet encryption scheme is a triple DES encryption, and further encrypts the packet header and the packet data.

11. A security system, as in claim 10, wherein:

the server further comprises means to encrypt a fourth logon packet with session information; and

the client further comprises means to decrypt the fourth logon packet.

12. A security system, as in claim 9, wherein:

the client further comprises means to encrypt data packets; and

the server further comprises means to encrypt data packets;

data packets are selectably encrypted using at least one of the security levels; and

means to dynamically adjust the size of the packet header based on the selected encryption scheme.

13. A security system, as in claim 5, wherein:

each client includes at least one application program; and

the server further comprises at least one packet queue for each client;

whereby application performance is improved by reducing packet search time.

14. A method of securely transmitting packet data between a client and a server with encrypted packets, including the steps of:

using at least one communication channel to transmit packets between at least one client machine and at least one server;

encrypting in the client a first logon packet;

transmitting the first logon packet to the server;

decrypting the first logon packet in the server;

encrypting a second logon packet in the server with client authenticating information;

transmitting the second logon packet to the client;

decrypting the second logon packet in the client;

encrypting in the client a third logon packet with session information;

decrypting the third logon packet in the server;

whereby the client and server can establish secure communications by bi-directionally transmitting encrypted data.

15. A method, as in claim 14, including the further steps of:

encrypting a fourth logon packet in the server with session information;

transmitting the fourth logon packet to the client; and

decrypting the fourth logon packet in the client;

using the session information to control encryption of packets while communicating between the client and the server.

16. A method, as in claim 15, including the further step of using at least two selectable encryption schemes, including a first encryption scheme for a first security level and a second encryption scheme for a second security level.

17. A method, as in claim 16, including the further steps of:

using at least two communication channels to communicate between multiple client and server, at least a first communication channel having a first level of security and at least a second communication channel having a second level of security; and

selecting the first encryption scheme for the first communication channel and the second encryption scheme for the second communication channel.

18. A method, as in claim 17, including the further step of using single DES encryption for the first level of security and triple DES encryption for the second level of security.

19. A method, as in claim 18, including the further steps of:

using packets which contain a header portion and a data portion; and

using a third encryption scheme in which triple DES encryption is used for the packet header and the packet data.

20. A method, as in claim 19, including the further steps of:

selecting the encryption scheme based on the nature of the data in the packet; and

dynamically adjusting the size of the packet header based on the selected encryption scheme.

* * * * *

US005878231A

United States Patent [19]

Baehr et al.

[11] **Patent Number:** 5,878,231

[45] **Date of Patent:** Mar. 2, 1999

[54] **SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE**

[75] Inventors: **Geoffrey G. Baehr**, Palo Alto; **William Danielson**, Mountain View; **Thomas L. Lyon**, Palo Alto, all of Calif.; **Geoffrey Mulligan**, Colorado Springs, Colo.; **Martin Patterson**, Grenoble, France; **Glenn C. Scott**, Mountain View; **Carolyn Turbyfill**, Los Gatos, both of Calif.

[73] Assignee: **Sun Microsystems, Inc.**, Palo Alto, Calif.

[21] Appl. No.: 795,374

[22] Filed: **Feb. 4, 1997**

Related U.S. Application Data

[62] Division of Ser. No. 444,351, May 18, 1995, Pat. No. 5,802,320.

[51] **Int. Cl.**[6] **G06F 13/38; G06F 15/17**

[52] **U.S. Cl.** **395/200.75**; 395/200.73

[58] **Field of Search** 370/401, 403; 395/200.7, 200.8, 200.71, 200.73, 200.75

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,577,313	3/1986	Sy	371/403
5,550,984	8/1996	Gelb	395/200.75
5,559,883	9/1996	Williams	380/4
5,590,285	12/1996	Krause et al.	395/200.48
5,606,668	2/1997	Shwed	395/187.01
5,623,601	4/1997	Vu	395/187.01

OTHER PUBLICATIONS

"Firewalls and Internet Security," by Cheswick & Bellovin, Addison Wesley, 1994.

"Firewall Routers and Packet Filtering," by Gary Kessler, Feb. 1995.

ip–masq.c from Linux kernel (v.2.0.27), 1994.

ip–fw.c from Linux kernel (v 2.0.27), 1994.

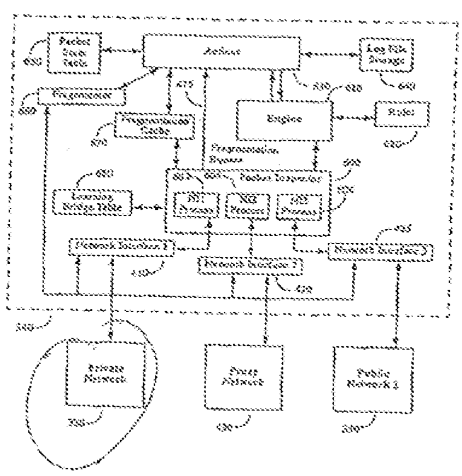
Primary Examiner—David L. Robertson

Attorney, Agent, or Firm—Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.

[57] **ABSTRACT**

A system for screening data packets transmitted between a network to be protected, such as a private network, and another network, such as a public network. The system includes a dedicated computer with multiple (specifically, three) types of network ports: one connected to each of the private and public networks, and one connected to a proxy network that contains a predetermined number of the hosts and services, some of which may mirror a subset of those found on the private network. The proxy network is isolated from the private network, so it cannot be used as a jumping off point for intruders. Packets received at the screen (either into or out of a host in the private network) are filtered based upon their contents, state information and other criteria, including their source and destination, and actions are taken by the screen depending upon the determination of the filtering phase. The packets may be allowed through, with or without alteration of their data, IP (internet protocol) address, etc., or they may be dropped, with or without an error message generated to the sender of the packet. Packets may be sent with or without alteration to a host on the proxy network that performs some or all of the functions of the intended destination host as specified by a given packet. The passing through of packets without the addition of any network address pertaining to the screening system allows the screening system to function without being identifiable by such an address, and therefore it is more difficult to target as an IP entity, e.g. by intruders.

12 Claims, 7 Drawing Sheets



US006332158B1

(12) **United States Patent**
Risley et al.

(10) **Patent No.:** **US 6,332,158 B1**
(45) **Date of Patent:** **Dec. 18, 2001**

(54) **DOMAIN NAME SYSTEM LOOKUP ALLOWING INTELLIGENT CORRECTION OF SEARCHES AND PRESENTATION OF AUXILIARY INFORMATION**

(76) Inventors: **Chris Risley**, 372 Stevick Dr., Atherton, CA (US) 94027; **Richard Lamb**, 11 Roxbury Ave., Natick, MA (US) 01760; **Eduard Guzovsky**, 11 Page Rd., Weston, MA (US) 02493

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/207,701**

(22) Filed: **Dec. 9, 1998**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/204,855, filed on Dec. 3, 1998, now abandoned.

(51) **Int. Cl.**[7] **G06F 13/00**
(52) **U.S. Cl.** **709/219**; 709/225; 709/313; 709/329
(58) **Field of Search** 709/217, 219, 709/223, 224, 225, 226, 227, 229, 313, 328, 329

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,855,020	*	12/1998	Kirsch	707/10
5,907,680	*	5/1999	Nielsen	707/533
6,041,041	*	3/2000	Ramanathan et al.	370/241
6,041,324	*	3/2000	Earl et al.	707/9
6,092,178	*	7/2000	Jindal et al.	712/27

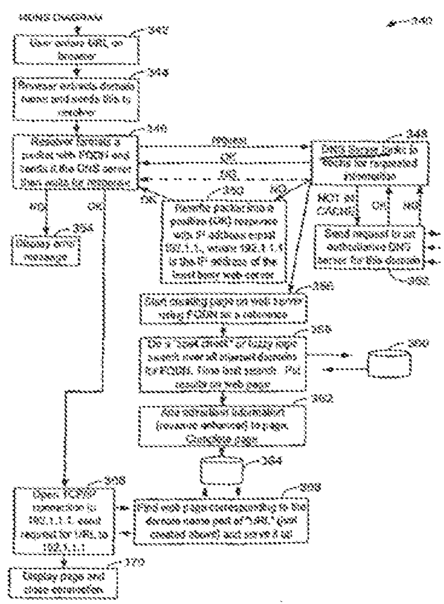
* cited by examiner

Primary Examiner—Viet D. Vu
(74) *Attorney, Agent, or Firm*—Townsend and Townsend and Crew LLP; Charles L. Kulas; Fidel D. Nwamu

(57) **ABSTRACT**

A domain name server assists user's in selecting desired domains in the Internet. A domain name query is sent from a resolver process, or equivalent process, when the user (or a process on the user's computer) wishes to obtain information. If the domain name exists, the domain name server provides the corresponding machine address back to the user's computer. However, when the domain name query uses a non-existent domain name then a machine address for a computer that executes a domain recommendation engine is returned instead of a machine address associated with the invalid domain. The domain recommendation engine assists the user (or process on the user's computer) in locating a desired domain name. The domain name recommendation engine can take into account numerous factors that assist in determining the intended domain, including common misspellings, phonetic errors, sub-domain errors, past statistics on website accessing by the present user and prior users. Auxiliary information is provided to the user along with information to assist in locating the intended domain. The auxiliary information can include sponsorship information, referrals, advertisements, educational or other information. The auxiliary information can be in the form of image, audio, database of other types of information.

22 Claims, 7 Drawing Sheets



US005898830A

United States Patent [19]

Wesinger, Jr. et al.

[11] **Patent Number:** **5,898,830**

[45] **Date of Patent:** **Apr. 27, 1999**

[54] **FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY**

[75] Inventors: **Ralph E. Wesinger, Jr.**, San Jose; **Christopher D. Coley**, Morgan Hill, both of Calif.

[73] Assignee: **Network Engineering Software**, San Jose, Calif.

[21] Appl. No.: **08/733,361**

[22] Filed: **Oct. 17, 1996**

[51] **Int. Cl.**[6] **G06F 1/00**

[52] **U.S. Cl.** **395/187.01**; 395/200.55; 395/200.57

[58] **Field of Search** 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,713,753	12/1987	Boebert et al.	364/200
4,799,153	1/1989	Hann et al.	380/25
4,799,156	1/1989	Shavit et al.	364/401
5,191,611	3/1993	Lang	380/25
5,241,594	8/1993	Kung	380/4
5,416,842	5/1995	Aziz	380/30

(List continued on next page.)

OTHER PUBLICATIONS

Kiuchi et al., "C-HTTP The Development of a Secure, Closed HTTP Based Network on the Internet", PRoceedings of SNDSS, IEEE, pp. 64–75, Jun. 1996.

Neuman, "Proxy Based Authorization and Accounting for Distributed Systems", IEEE, pp. 283–291, 1993.

Network Firewalls; *IEEE Communications Magazine*; (Bellovin et al.) pp. 50–57; Sep., 1994.

The MITRE Security Perimeter; *IEEE Communications Magazine*; (Goldberg); pp. 212–218; 1994.

IpAccess—An Internet Service Access System for Firewall Installations; *IEEE Communications Magazine*; (Stempel); pp. 31–41; 1995.

Remote Control of Diverse Network Elements Using SNMP; *IEEE Communications Magazine*; (Aicklen et al.); pp. 673–667; 1995.

Firewall's Information is Money!, *Scientific Management Corporation.*

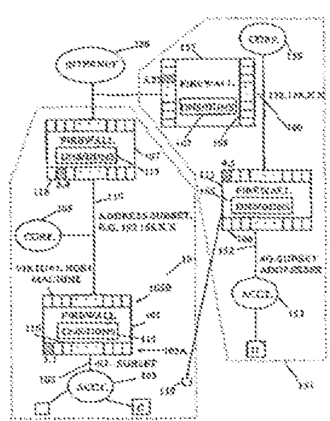
Primary Examiner—Joseph Palys

Attorney, Agent, or Firm—McDonnell Boehnen Hulbert & Berghoff

[57] **ABSTRACT**

The present invention, generally speaking, provides a firewall that achieves maximum network security and maximum user convenience. The firewall employs "envoys" that exhibit the security robustness of prior-art proxies and the transparency and ease-of-use of prior-art packet filters, combining the best of both worlds. No traffic can pass through the firewall unless the firewall has established an envoy for that traffic. Both connection-oriented (e.g., TCP) and connectionless (e.g., UDP-based) services may be handled using envoys. Establishment of an envoy may be subjected to a myriad of tests to "qualify" the user, the requested communication, or both. Therefore, a high level of security may be achieved. The usual added burden of prior-art proxy systems is avoided in such a way as to achieve full transparency-the user can use standard applications and need not even know of the existence of the firewall. To achieve full transparency, the firewall is configured as two or more sets of virtual hosts. The firewall is, therefore, "multi-homed," each home being independently configurable. One set of hosts responds to addresses on a first network interface of the firewall. Another set of hosts responds to addresses on a second network interface of the firewall. In one aspect, programmable transparency is achieved by establishing DNS mappings between remote hosts to be accessed through one of the network interfaces and respective virtual hosts on that interface. In another aspect, automatic transparency may be achieved using code for dynamically mapping remote hosts to virtual hosts in accordance with a technique referred to herein as dynamic DNS, or DDNS.

21 Claims, 9 Drawing Sheets



VNET00222006

US006079020A

United States Patent [19]

Liu

[11] **Patent Number: 6,079,020**

[45] **Date of Patent: Jun. 20, 2000**

[54] METHOD AND APPARATUS FOR MANAGING A VIRTUAL PRIVATE NETWORK

[75] Inventor: **Quentin C. Liu**, Cupertino, Calif.

[73] Assignee: **VPNet Technologies, Inc.**, Milpitas, Calif.

[21] Appl. No.: **09/013,743**

[22] Filed: **Jan. 27, 1998**

[51] **Int. Cl.**^{7} **G06F 11/30**

[52] **U.S. Cl.** **713/201**; 709/223

[58] **Field of Search** 713/200, 201; 709/220–226

[56] **References Cited**

U.S. PATENT DOCUMENTS

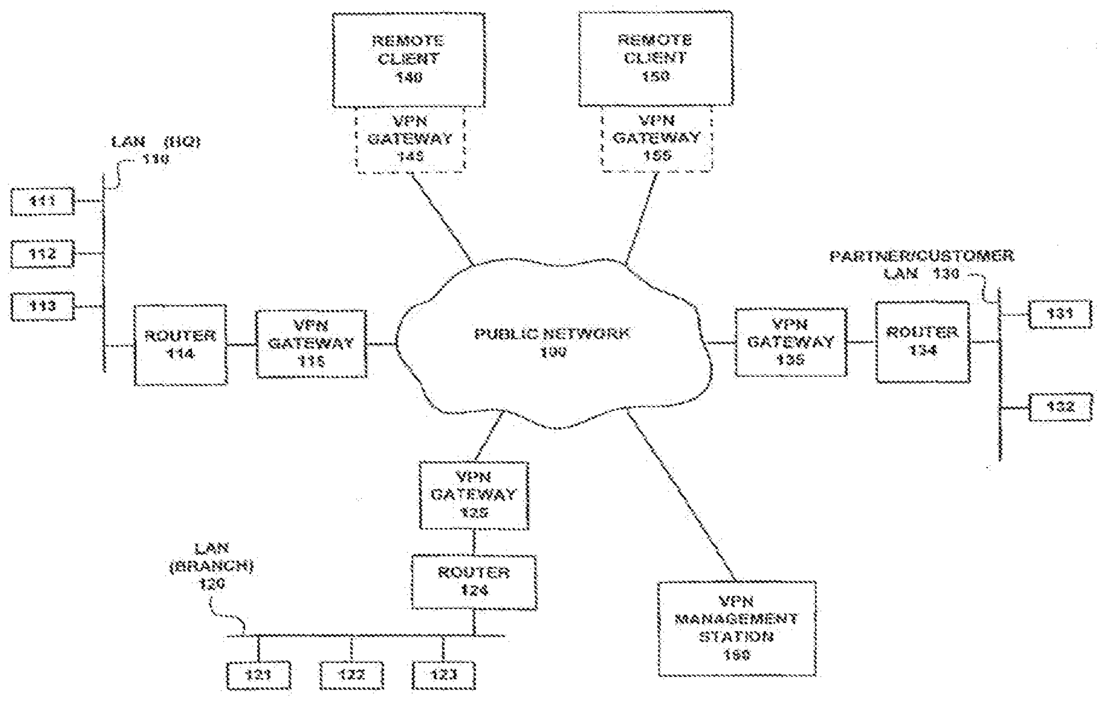
5,339,356	8/1994	Ishii	379/234
5,432,783	7/1995	Ahmed et al.	370/60.1
5,490,212	2/1996	Lautenschlager	379/225
5,504,921	4/1996	Dev et al.	395/800
5,550,816	8/1996	Hardwick et al.	370/60
5,623,601	4/1997	Vu	395/187.01
5,659,542	8/1997	Bell et al.	370/496
5,742,762	4/1998	Scholl et al.	395/200.3
5,768,271	6/1998	Seid et al.	370/389
5,799,016	8/1998	Onweller	370/401
5,898,830	4/1999	Wesinger, Jr. et al.	395/187.01

Primary Examiner—Ayaz R. Sheikh
Assistant Examiner—Jigar Pancholi
Attorney, Agent, or Firm—Park & Vaughan LLP

[57] **ABSTRACT**

The present invention provides a method and an apparatus for managing a virtual private network operating over a public data network. This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways. One embodiment of the present invention includes a system that operates by receiving a command specifying an operation on the virtual private network. The system determines which virtual private network gateways are affected by the command. The system then automatically translates the command into configuration parameters for virtual private network gateways affected by the command. These configuration parameters specifying how the virtual private network gateways handle communications between specific groups of addresses on the public data network. The system then transmits the configuration parameters to the virtual private network gateways affected by the command, so that the virtual private network gateways are configured to implement the command.

22 Claims, 11 Drawing Sheets



US006330562B1

(12) **United States Patent**
Boden et al.

(10) **Patent No.:** **US 6,330,562 B1**
(45) **Date of Patent:** **Dec. 11, 2001**

(54) **SYSTEM AND METHOD FOR MANAGING SECURITY OBJECTS**

(75) Inventors: **Edward B. Boden; Franklin A. Gruber**, both of Vestal; **Mark J. Melville**, Endwell; **Frank V. Paxhia**, Binghamton; **Michael D. Williams**, Owego, all of NY (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/239,693**

(22) Filed: **Jan. 29, 1999**

(51) **Int. Cl.**[7] **G06F 17/30**
(52) **U.S. Cl.** **707/10**; 707/9; 709/220; 713/200; 713/201; 713/202
(58) **Field of Search** 707/9–10; 713/200–202; 709/220

(56) **References Cited**

U.S. PATENT DOCUMENTS

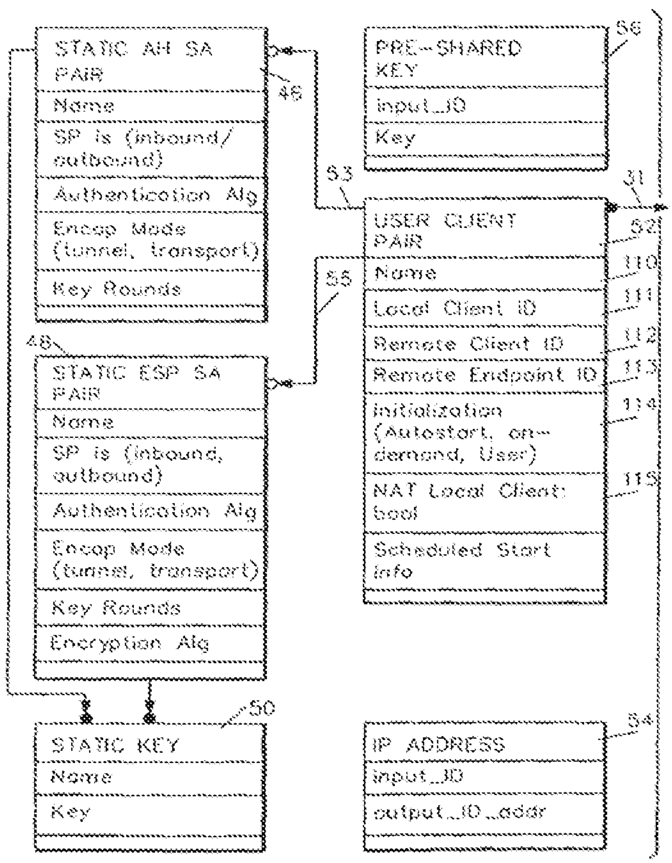
5,051,982	9/1991	Brown et al.	370/58.2
5,621,727	4/1997	Vaudreuil	370/60
5,764,909	6/1998	Nishimura	395/200.93
5,768,271	6/1998	Seid et al.	370/389
5,835,726	11/1998	Shwed et al.	395/200.59
5,842,043	11/1998	Nishimura	395/856

Primary Examiner—Hosain T. Alam
Assistant Examiner—Camy Truong
(74) *Attorney, Agent, or Firm*—Shelley M Beckstrand

(57) **ABSTRACT**

A data model for abstracting customer-defined VPN security policy information. By employing this model, a VPN node (computer system existing in a Virtual Private Network) can gather policy configuration information for itself through a GUY, or some distributed policy source, store this information in a system-defined database, and use this information to dynamically negotiate, create, delete, and maintain secure connections at the IP level with other VPN nodes.

15 Claims, 6 Drawing Sheets



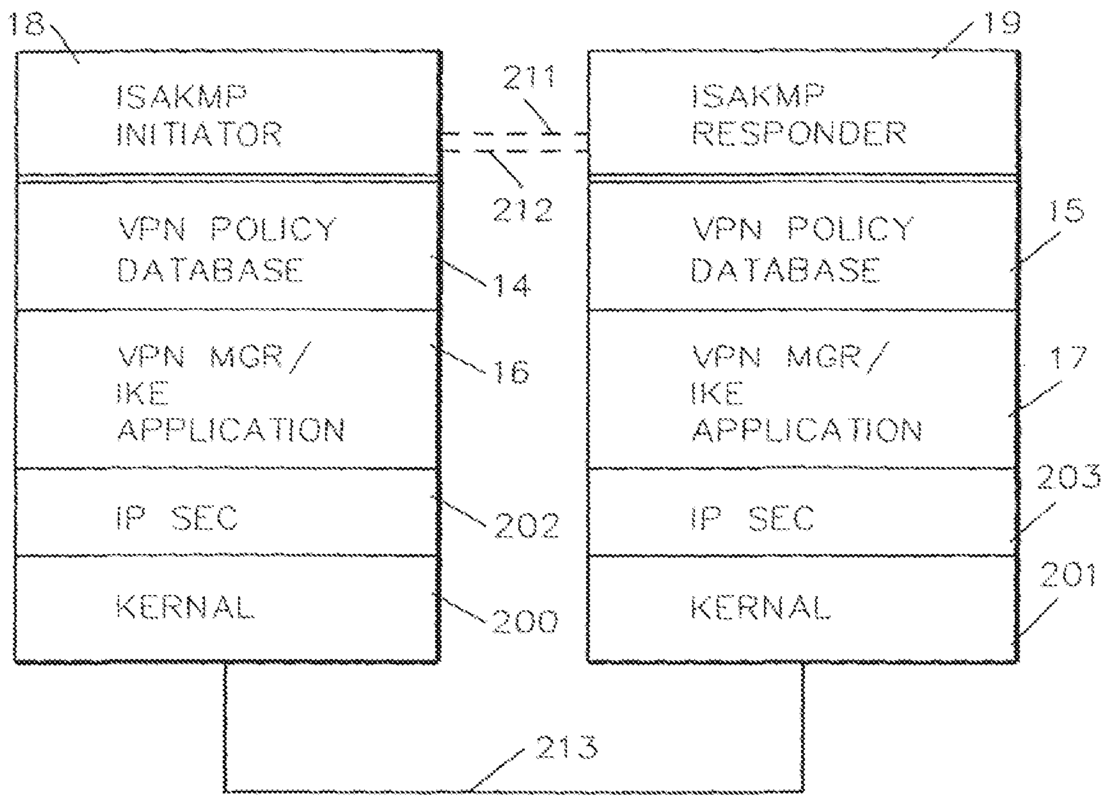

18
ISAKMP
INITIATOR
211
212
19
ISAKMP
RESPONDER
VPN POLICY
DATABASE
14
VPN POLICY
DATABASE
15
VPN MGR/
IKE
APPLICATION
16
VPN MGR/
IKE
APPLICATION
17
IP SEC
202
IP SEC
203
KERNAL
200
KERNAL
201
213

FIG. 1

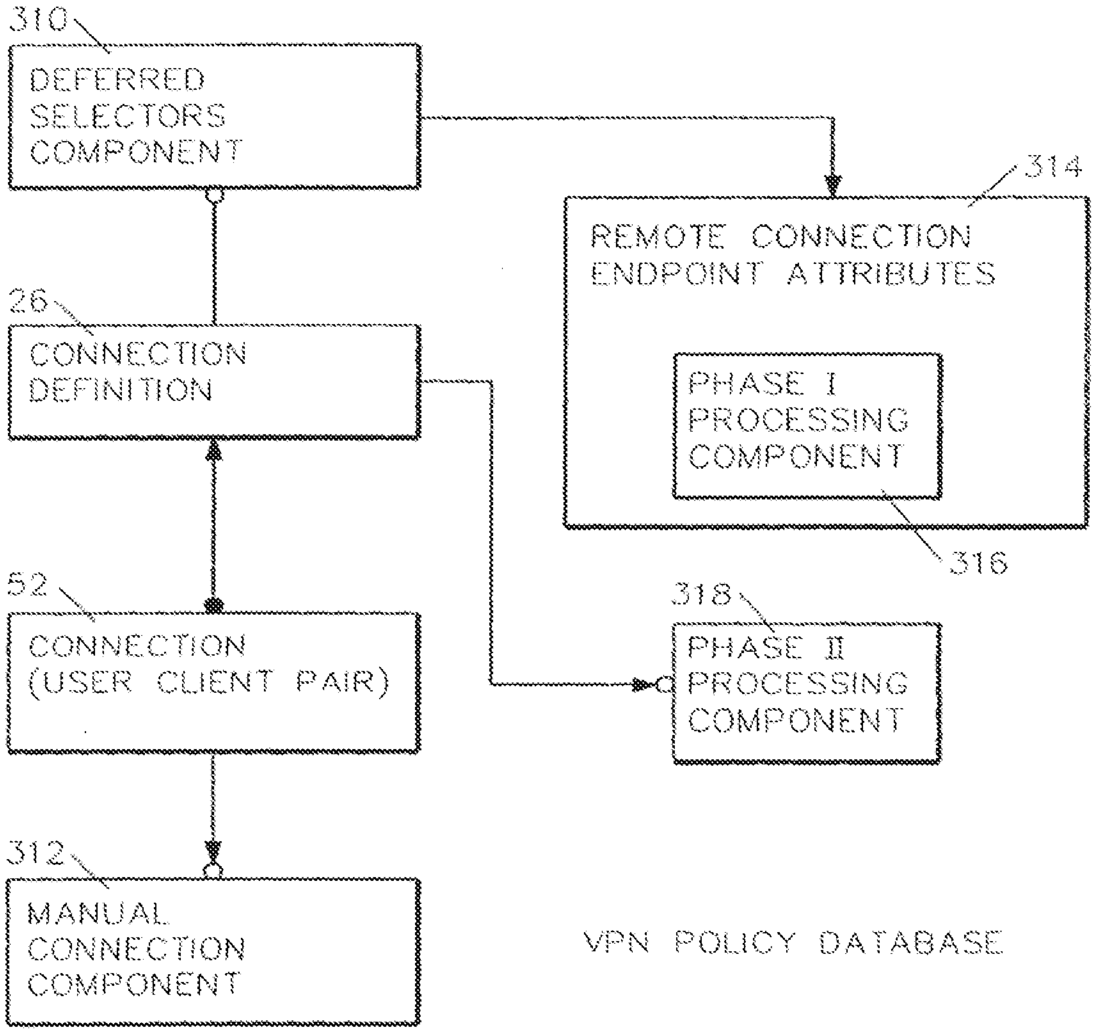

310
DEFERRED SELECTORS COMPONENT
314
REMOTE CONNECTION ENDPOINT ATTRIBUTES
26
CONNECTION DEFINITION
PHASE I PROCESSING COMPONENT
316
52
318
CONNECTION (USER CLIENT PAIR)
PHASE II PROCESSING COMPONENT
312
MANUAL CONNECTION COMPONENT
VPN POLICY DATABASE

FIG. 2

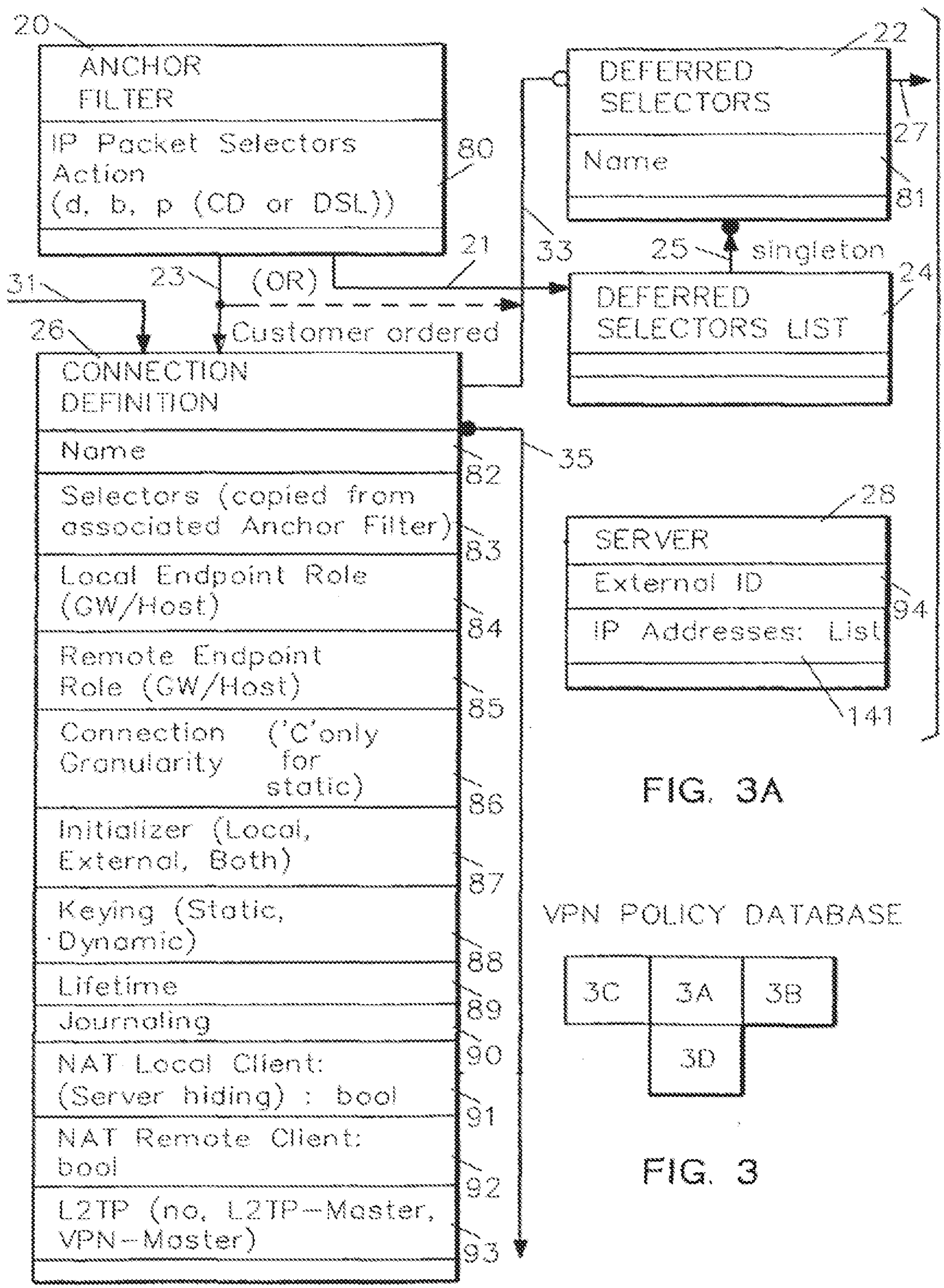


FIG. 3A

VPN POLICY DATABASE

FIG. 3

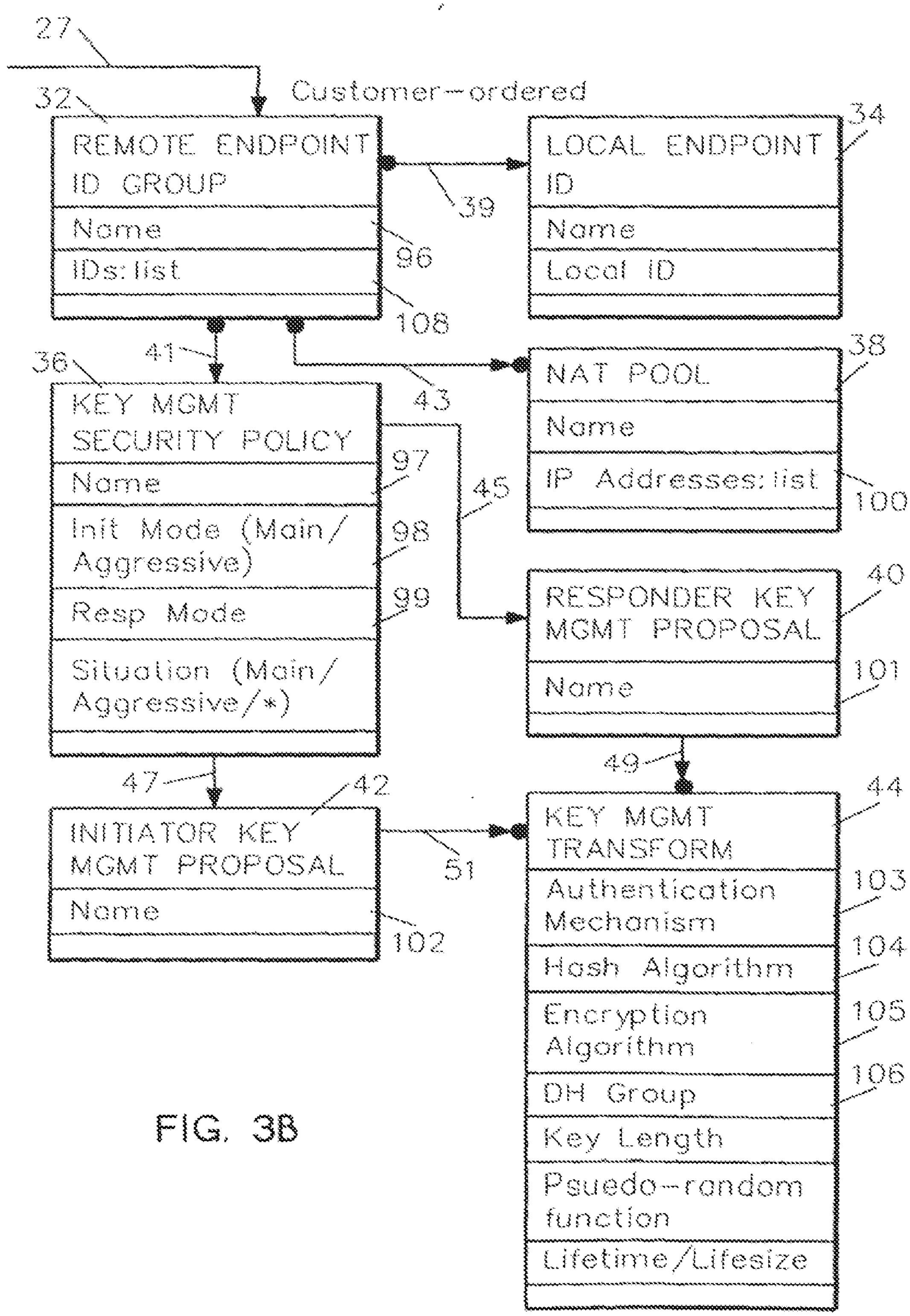

27
Customer-ordered
32
REMOTE ENDPOINT ID GROUP
Name
IDs: list
34
LOCAL ENDPOINT ID
Name
Local ID
39
96
108
36
41
38
NAT POOL
Name
IP Addresses: list
43
KEY MGMT SECURITY POLICY
Name
Init Mode (Main/ Aggressive)
Resp Mode
Situation (Main/ Aggressive/*)
97
98
99
45
100
40
RESPONDER KEY MGMT PROPOSAL
Name
101
49
47
42
44
INITIATOR KEY MGMT PROPOSAL
Name
51
102
KEY MGMT TRANSFORM
Authentication Mechanism
Hash Algorithm
Encryption Algorithm
DH Group
Key Length
Psuedo-random function
Lifetime/Lifesize
103
104
105
106

FIG. 3B

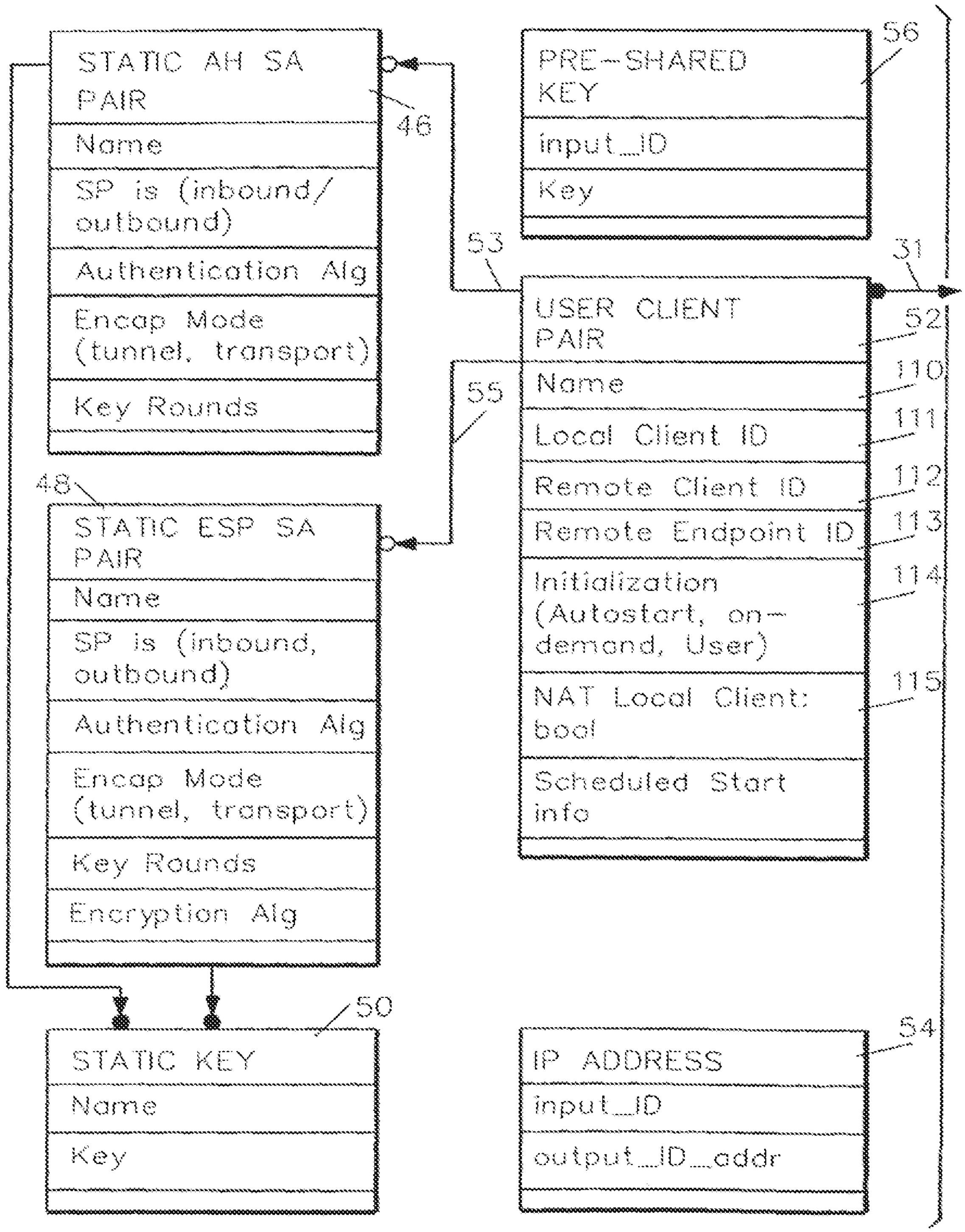
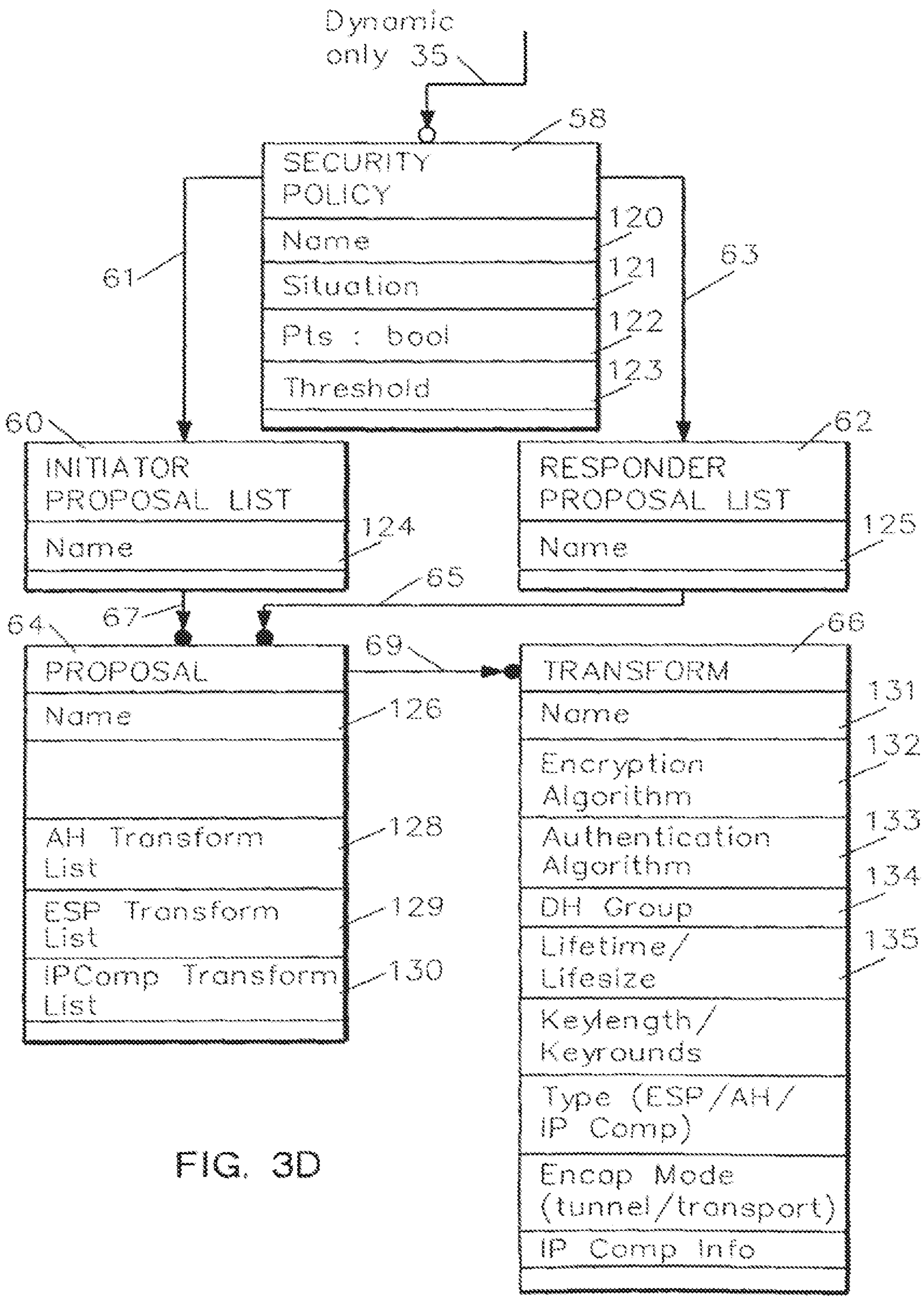

STATIC AH SA PAIR
Name
SP is (inbound/ outbound)
Authentication Alg
Encap Mode (tunnel, transport)
Key Rounds
46
PRE-SHARED KEY
input_ID
Key
56
53
31
USER CLIENT PAIR
Name
Local Client ID
Remote Client ID
Remote Endpoint ID
Initialization (Autostart, on-demand, User)
NAT Local Client: bool
Scheduled Start info
52
110
111
112
113
114
115
55
48
STATIC ESP SA PAIR
Name
SP is (inbound, outbound)
Authentication Alg
Encap Mode (tunnel, transport)
Key Rounds
Encryption Alg
50
STATIC KEY
Name
Key
54
IP ADDRESS
input_ID
output_ID_addr

FIG. 3C



Dynamic
only 35
58
SECURITY
POLICY
Name
Situation
Pts : bool
Threshold
120
121
122
123
61
63
60
INITIATOR
PROPOSAL LIST
Name
124
62
RESPONDER
PROPOSAL LIST
Name
125
65
67
64
PROPOSAL
Name
126
AH Transform
List
128
ESP Transform
List
129
IPComp Transform
List
130
69
66
TRANSFORM
Name
131
Encryption
Algorithm
132
Authentication
Algorithm
133
DH Group
134
Lifetime/
Lifesize
135
Keylength/
Keyrounds
Type (ESP/AH/
IP Comp)
Encap Mode
(tunnel/transport)
IP Comp Info

FIG. 3D

4. Checking those attributes of the client ID pair for which the granularity 86 indicates 'single' or 'client' against the local endpoint role 84 and remote endpoint role 85, as shown in Table 2; and
5. Using the client ID pair and the connection definition selectors 83 to generate the connection client IDs according to the connection granularity; 'client' or 'single' indicate the value comes from the client ID pair, 'filter' indicates the value comes from the connection definition selectors 83.

The resulting connection client IDs are then used to create the filter rules (SPD entry) for this connection in the kernal.

Advantages over the Prior Art

It is a further advantage of the invention that there is provided a system and method for creating, maintaining, deleting and retrieving VPN policy objects.

It is a further advantage of the invention that there is provided a system and method for enabling acceptance of previously unknown IDci/IDcr values from a remote system.

It is a further advantage of the invention that there is provided a system and method enabling dynamic generation, load, and management of multiple IPSec filter rules.

It is a further advantage of the invention that there is provided a system and method enabling ISAKMP phase II driven phase I connections.

It is a further advantage of the invention that there is provided a system and method enabling handling of remote initiating hosts with dynamically assigned IP addresses with differing security policy requirements.

It is a further advantage of the invention that there is provided flexibility in policy definition in the areas of dynamically-assigned IP addresses, remotely-defined ISAKMP client IDs (IDci/IDcr), and separation of ISAKMP Phase I (key management) policy information from ISAKMP Phase II (data management) policy information.

It is a further advantage of the invention that there is provided a data model for representing and abstracting IPSec/ISAKMP-based VPN configuration information for an IPSec-capable computer system in a virtual private network that (1) allows for each customer-generated customer-ordered security policy database (SPD) entry, multiple VPN connections to be dynamically established (these connections may or may not have been previously defined); (2) allows for a data-security-policy-driven approach to rekeying (via IKE) where (a) the key management connection (i.e. the secure connection used to exchange keying material for the data connections) is created and maintained by security policy and on an on-demand basis by data connection activity, and (b) the key connection security policy is determined solely by the identity of the remote connection endpoint; (3) allows for dynamically establishing VPN connections with different security policies and other attributes, based solely on an unfixed IP address (e.g. a user ID)—these connections may or may not have been previously defined. This aspect is used for supporting systems with dynamically-assigned IP addresses that wish to establish a VPN connection with the local system.

Alternative Embodiments

It will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without departing from the spirit and scope of the invention. In particular, it is within the scope of the invention to provide a program storage or memory device such as a solid or fluid transmission medium, magnetic or optical wire, tape or disc, or the like, for storing signals readable by a machine for controlling the operation of a computer according to the method of the invention and/or to structure its components in accordance with the system of the invention.

Accordingly, the scope of protection of this invention is limited only by the following claims and their equivalents.

We claim:

1. A policy database system for managing security objects, comprising:

a deferred selectors component;

a connection definition;

a user client pair;

a manual connection component;

a remote connection endpoint attributes component including a phase I processing component; and

a phase II processing component;

said connection definition having a zero or one reference relationship with said deferred selectors component, a zero or more reference relationship with said user client pair, and a zero or one reference relationship with said phase II processing component, said user client pair further having a zero or one reference relationship with said manual connection component; and said deferred selectors component having a one and only one reference relationship with said remote connection attributes component.

2. The policy database system of claim 1 further for enabling acceptance at a responder node of a previously unknown client ID pair from an initiator node, said connection definition comprising indicia for determining if said unknown client pair is acceptable to said responder node and said phase II processing component comprising a policy for negotiating said unknown client ID pair.

3. The policy database system of claim 1 further for enabling dynamic generation, loading and management of multiple connection filters, said connection definition being selectable selectively by said user client pair or a client ID pair received from a remote initiator node for identifying pertinent granularity attributes defining the subset of datagrams that can be associated with any one connection instantiated from said connection definition.

4. The policy database system of claim 1 further for enabling ISAKMP phase II driven phase I connections, said remote connection endpoints attributes further comprising a remote endpoint identifier and a reference pointer for associating said remote endpoint identifier with a phase I negotiation policy in said phase I processing component.

5. The policy database system of claim 1 further for enabling secure connection by a responder node to a remote initiating host with dynamically assigned IP address, further comprising:

an anchor filter for defining datagrams that may be associated with remote hosts using dynamically assigned IP addresses;

said deferred selectors component further providing a one to many mapping from said anchor filter to said connection definitions.

6. A method for managing a policy database, said database including a deferred selectors component, a connection definition, a user client pair, a manual connection component, a remote connection endpoint attributes component including a phase I processing component; and a phase II processing component, comprising the steps of:

maintaining a zero or one reference relationship of said connection definition with said deferred selectors component;

maintaining a zero or more reference relationship of said connection definition with said user client pair;

maintaining a zero or one reference relationship of said connection definition with said phase II processing component;

maintaining a zero or one reference relationship of said user client pair with said manual connection component; and

maintaining a one and only one reference relationship of said deferred selectors component with said remote connection attributes component.

7. The method of claim 6, further for enabling acceptance at a responder node of a previously unknown client ID pair from an initiator node, comprising the further steps of:

determining from connection definition indicia if said unknown client pair is acceptable to said responder node, and if so

obtaining from said phase II processing component a policy for negotiating said unknown client ID pair.

8. The method of claim 6, further for enabling dynamic generation, load and management of multiple connection filters, comprising the further steps of:

obtaining from a said connection definition, selectively selected by said user client pair or a client ID pair received from a remote initiator node, granularity attributes defining the subset of datagrams that can be associated with any one connection instantiated from said connection definition.

9. The method of claim 6, further for enabling ISAKMP phase II driven phase I connections, comprising the further steps of:

associating a remote endpoint identifier in said remote connection endpoints attributes with a phase I negotiation policy in said phase I processing component.

10. The method of claim 6, further for enabling secure connection by a responder node to a remote initiating host with dynamically assigned IP address, further comprising the steps of:

providing an anchor filter for defining datagrams that may be associated with remote hosts using dynamically assigned IP addresses; and

said deferred selectors component further providing a one to many mapping from said anchor filter to said connection definitions.

11. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for managing a policy database, said database including a deferred selectors component, a connection definition, a user client pair, a manual connection component, a remote connection endpoint attributes component including a phase I processing component; and a phase II processing component, said method steps comprising:

maintaining a zero or one reference relationship of said connection definition with said deferred selectors component;

maintaining a zero or more reference relationship of said connection definition with said user client pair;

maintaining a zero or one reference relationship of said connection definition with said phase II processing component;

maintaining a zero or one reference relationship of said user client pair with said manual connection component; and

maintaining a one and only one reference relationship of said deferred selectors component with said remote connection attributes component.

12. An article of manufacture comprising:

a computer useable medium having computer readable program code means embodied therein for managing a policy database, said database including a deferred selectors component, a connection definition, a user client pair, a manual connection component, a remote connection endpoint attributes component including a phase I processing component; and a phase II processing component, the computer readable program means in said article of manufacture comprising:

computer readable program code means for causing a computer to effect maintaining a zero or one reference relationship of said connection definition with said deferred selectors component;

computer readable program code means for causing a computer to effect maintaining a zero or more reference relationship of said connection definition with said user client pair;

computer readable program code means for causing a computer to effect maintaining a zero or one reference relationship of said connection definition with said phase II processing component;

computer readable program code means for causing a computer to effect maintaining a zero or one reference relationship of said user client pair with said manual connection component; and

computer readable program code means for causing a computer to effect maintaining a one and only one reference relationship of said deferred selectors component with said remote connection attributes component.

13. A policy database system for managing security objects and enabling ISAKMP phase II driven phase I connections, comprising:

a deferred selectors component;

a connection definition;

a user client pair;

a manual connection component;

a remote connection endpoint attributes component including a phase I processing component; and

a phase II processing component;

said connection definition having a zero or one reference relationship with said deferred selectors component, a zero or more reference relationship with said user client pair, and a zero or one reference relationship with said phase II processing component; said user client pair further having a zero or one reference relationship with said manual connection component; and said deferred selectors component having a one and only one reference relationship with said remote connection attributes component; and

said remote connection endpoints attributes further comprising a remote endpoint identifier and a reference pointer for associating said remote endpoint identifier with a phase I negotiation policy in said phase I processing component.

14. A method for managing a policy database and enabling ISAKMP phase II driven phase I connections, said database including a deferred selectors component, a connection definition, a user client pair, a manual connection component, a remote connection endpoint attributes component including a phase I processing component; and a phase II processing component, comprising the steps of:

maintaining a zero or one reference relationship of said connection definition with said deferred selectors component;

maintaining a zero or more reference relationship of said connection definition with said user client pair;

maintaining a zero or one reference relationship of said connection definition with said phase II processing component;

maintaining a zero or one reference relationship of said user client pair with said manual connection component;

maintaining a one and only one reference relationship of said deferred selectors component with said remote connection attributes component; and

associating a remote endpoint identifier in said remote connection endpoints attributes with a phase I negotiation policy in said phase I processing component.

15. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for managing a policy database and enabling ISAKMP phase II driven phase I connections, said database including a deferred selectors component, a connection definition, a user client pair, a manual connection component, a remote connection endpoint attributes component including a phase I processing component; and a phase II processing component, said method steps comprising:

maintaining a zero or one reference relationship of said connection definition with said deferred selectors component;

maintaining a zero or more reference relationship of said connection definition with said user client pair;

maintaining a zero or one reference relationship of said connection definition with said phase II processing component;

maintaining a zero or one reference relationship of said user client pair with said manual connection component;

maintaining a one and only one reference relationship of said deferred selectors component with said remote connection attributes component; and

associating a remote endpoint identifier in said remote connection endpoints attributes with a phase I negotiation policy in said phase I processing component.

* * * * *

US006081900A

United States Patent [19]

Subramaniam et al.

[11] Patent Number: 6,081,900
[45] Date of Patent: Jun. 27, 2000

[54] SECURE INTRANET ACCESS

[75] Inventors: Anand Subramaniam, San Jose, Calif.; Hashem M. Ebrahimi, Salt Lake City, Utah

[73] Assignee: Novell, Inc., Provo, Utah

[21] Appl. No.: 09/268,795

[22] Filed: Mar. 16, 1999

[51] Int. Cl.[7] H04L 9/32; G06F 13/38

[52] U.S. Cl. 713/201; 713/153; 707/10; 707/513; 709/230; 709/245

[58] Field of Search 713/151, 153, 713/155, 160, 162, 201; 709/217, 218, 214, 230, 238, 245; 707/10, 501, 513

[56] References Cited

U.S. PATENT DOCUMENTS

5,522,041	5/1996	Murakami et al.	709/203
5,550,984	8/1996	Gelb	395/200.17
5,553,239	9/1996	Heath et al.	395/187.01
5,673,322	9/1997	Pepe et al.	380/49
5,706,434	1/1998	Kremen et al.	709/218
5,727,145	3/1998	Nessett et al.	713/200
5,745,360	4/1998	Leone et al.	707/513
5,752,022	5/1998	Chiu et al.	707/10
5,757,924	5/1998	Friedman et al.	713/162
5,761,683	6/1998	Logan et al.	707/513
5,768,271	6/1998	Seid et al.	370/389
5,805,803	9/1998	Birrell et al.	713/201
5,825,890	10/1998	Elgamal et al.	380/49
5,890,171	3/1999	Blumer et al.	707/501
5,913,025	6/1999	Higley et al.	713/201
5,991,810	11/1999	Shapiro et al.	709/229

OTHER PUBLICATIONS

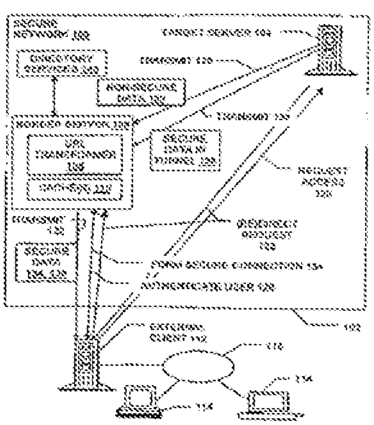
Andrew S. Tanenbaum, *Computer Networks*, 3d. Ed. (1996), pp. 28–39, 396–417, 601–621, 681–695.
"Securing Communications on the Intranet and Over the Internet", Netscape Communications Corporation (Jul. 1996), pp. 1–12.
"WebSTAR/SSL Security Toolkit: Troubleshooting", no later than Aug. 4, 1998, pp. 1–2.
Paul Ferguson, "What is a VPN?", Apr. 1998, pp. 1–22.
Virtual Private Networking: An Overview, no later than Jun. 25, 1998, pp. 1–20.
"How the proxy works", Jul. 22, 1998, pp. 1–2.
Microsoft Proxy Server Marketing Bulletin, 1998, pp. 1–8.
Microsoft Proxy Server What's New, 1998, pp. 1–4.
"CSM Proxy Server White Paper", 1995–1998, pp. 1–13.
"CSM Proxy Server, the Ultimate Gateway to the Internet!", no later than Aug. 4, 1998, pp. 1–5.
Qun Zhong et al., "Security Control for COTS Components", Jun. 1998 IEEE Computer, pp. 67–73.
"r[3] CypherClient Information", 1998, pp. 1–4.
NetSafe V3.0 The Firewall Solution from Siemens Nixdorf, May 31, 1997, pp. 1–3.
Submission: HTTPS v1.0 Package for OmniWeb 3.x (Rhapsody), Jan. 24, 1998, pp. 1–3.
OWF basics, Mar. 31, 1997, pp. 1–2.
"info needed to write https proxy", Apr. 11, 1996.
Webroute 1.3.0, May 28, 1997, pp. 1–2.
Werner Feibel, *Novell's Complete Encyclopedia of Networking*, 1995, pp. 625–630.
Bruce Schneier, *Applied Cryptography*, 1994, pp. 436–437.
"A New Management and Security Architecture for Extranets", 1996–1999, pp. 1–14.
Netscape Proxy Server Administrator's Guide, 1997, Contents, Introduction, and Chapters 1–17.

Primary Examiner—Gilberto Barrón, Jr.
Attorney, Agent, or Firm—Computer Law++

[57] ABSTRACT

Methods, signals, devices, and systems are provided for secure access to a network from an external client. Requests for access to confidential data may be redirected from a target server to a border server, after which a secure sockets layer connection between the border server and the external client carries user authentication information. After the user is authenticated to the network, requests may be redirected back to the original target server. Web pages sent from the target server to the external client are scanned for non-secure URLs such as those containing "http://" and modified to make them secure. The target server and the border server utilize various combinations of secure and non-secure caches. Although tunneling may be used, the extensive configuration management burdens imposed by virtual private networks are not required.

30 Claims, 4 Drawing Sheets



SN 7112690

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 (7) OF (7) PART(S)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 00479.00028	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/US 01/13260	International filing date *(day/month/year)* 25/04/2001	(Earliest) Priority Date *(day/month/year)* 30/10/1998
Applicant SCIENCE APPLICATIONS INTERNATIONAL CORPORATION		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 6 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [X] **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

   [ ] the text is approved as submitted by the applicant.

   [X] the text has been established by this Authority to read as follows:

   SECURE DOMAIN NAME SERVICE

5. With regard to the **abstract**,

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 26

   [ ] as suggested by the applicant.

   [X] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

Form PCT/ISA/210 (first sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/13260

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/12 H04L29/06 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DONALD E. EASTLAKE 3RD: "<draft-ietf-dnssec-secext2-05.txt> Domain Name System Security Extensions" INTERNET DRAFT, 'Online! April 1998 (1998-04), XP002199931 Retrieved from the Internet: <URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt> 'retrieved on 2002-05-23! 1. Overview of the contents 2.3 Data origin authemtication and integrity 2.4 DNS transaction and request authentication ----- -/--	1,4-6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 August 2002	23. 08. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertolissi, E

3

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/13260

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	CHAPMAN D.B.; ZWICKY E.D.: " Building Internet Firewalls" O'REILLY, November 1995 (1995-11), XP002199932 pag 278-296 pag 351-375	1,4-6
P,X	DE 199 24 575 A (SUN MICROSYSTEMS INC) 2 December 1999 (1999-12-02) abstract column 2, line 48 -column 3, line 6	1,4,5,7
A	P. SRISURESH, G. TSIRTSIS, P. AKKIRAJU, A. HEFFERNAN: "<draft-ietf-nat-dns-alg-00.txt> DNS extensions to Network Address Translators (DNS_ALG)" INTERNET DRAFT, 'Online! July 1998 (1998-07), XP002199933 Retrieved from the Internet: <URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-nat-dns-alg-00.txt> 'retrieved on 2002-05-23! 1. Introduction 2. Requirement for DNS extensions fig 3 5.3 Incoming name lookup queries 8. Security considerations	1-12
A	EP 0 838 930 A (DIGITAL EQUIPMENT CORP) 29 April 1998 (1998-04-29) abstract column 9, line 11 -column 10, line 34	1-12
X	JAMES E. BELLAIRE: "Subject: New Statement of Rules - Naming Internet Domains " INTERNET NEWSGROUP, 'Online! 30 July 1995 (1995-07-30), XP002209580 comp.dcom.telecom Retrieved from the Internet: <URL:http://groups.google.com/> 'retrieved on 2002-08-12! page 1, paragraph 8 page 2, paragraph 4	13,15
A	CLARK D: "US CALLS FOR PRIVATE DOMAIN-NAME SYSTEM" COMPUTER, IEEE COMPUTER SOCIETY, LONG BEACH., CA, US, US, vol. 31, no. 8, 1 August 1998 (1998-08-01), pages 22-25, XP000780513 ISSN: 0018-9162 page 22	13-16

-/--

3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

International Application No
PCT/US 01/13260

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	BEQUAI A: "Balancing Legal Concerns Over Crime and Security in Cyberspace" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 17, no. 4, 1998, pages 293-298, XP004129224 ISSN: 0167-4048 pag 296-297 Lanham Act	13-16
A	RICH WINKEL : "CAQ: NETWORKING WITH SPOOKS: THE NET & THE CONTROL OF INFORMATION " INTERNMET NEWSGROUP, 'Online! 21 June 1997 (1997-06-21), XP002209581 misc.activism.progressive Retrieved from the Internet: <URL:http://groups.google.com/> 'retrieved on 2002-08-12! the whole document	13-16

3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/13260

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. [ ] Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. [X] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[X] No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

International Application No. PCT/US 01 43260

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-12

   A portal for authenticating a query for a secure computer network address

2. Claims: 13-16

   A method and a computer readable storage medium for registering a secure domain name

IN'TERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/13260

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19924575 A	02-12-1999	DE 19924575 A1	02-12-1999
		FR 2782873 A1	03-03-2000
		GB 2340702 A ,B	23-02-2000
		JP 2000049867 A	18-02-2000
EP 0838930 A	29-04-1998	US 6101543 A	08-08-2000
		EP 0838930 A2	29-04-1998
		JP 10178450 A	30-06-1998

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 11/00
US CL : 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/201,200,202; 340/825.31,825.34; 380/255;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS US PATENT FILE; WEST; JPAB; EPAB; DWPI; TDBD;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,805,801 A (HOLLOWAY ET AL) 08 SEPTEMBER 1998, Entire document.	1-25
Y	US 5,796,942 A (ESBENSEN) 18 AUGUST 1998, Entire document.	1-25
Y,P	US 5,905,859 A (HOLLOWAY ET AL) 18 MAY 1999, Entire document.	1-25
Y	US 5,892,903 A (KLAUS) 06 APRIL 1999, Entire document.	1-25
A	US 5,537,099 A (LIANG) 16 JULY 1996, Entire document.	1-25
A	US 5,278,901 A (SHIEH ET AL) 11 JANUARY 1994, Entire document.	1-25

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 JULY 2000	22 AUG 2000

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	NADEEM IQBAL
Facsimile No. (703) 305-3230	Telephone No. (703) 308-5228

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,881 A (CONKLIN ET AL) 23 NOVEMBER 1999, Entire document.	1-25

Form PCT/ISA/210 (continuation of second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/02565

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/46, H04L 12/56, H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G09F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5898830 A (R.E.WESINGER, JR. ET AL), 27 April 1999 (27.04.99), column 3, line 47 - column 4, line 52, figure 1, claims 1-10, abstract, cited in Application --	1-20
A	C. HUITEMA: An Experiment in DNS BasedIP Routing. K B Labs Kashpureff Boling Laboratories, Inc., Network Working Group, rfc 1383, INRIA dec. 1992. http:www.kblabs.com/lab/lib/rfcs/1300/rfc1383.txt.html --	1-20
A	WO 9859470 A2 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 30 December 1998 (30.12.98), page 1, line 13 - page 3, line 16, figures 1-2, claims 1-12 --	1,20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 17 April 2001	Date of mailing of the international search report 18 -04- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Roger Bou Faisal/LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

25/02/01

International application No.
PCT/SE 00/02565

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5898830 A	27/04/99	US 6052788 A	18/04/00
WO 9859470 A2	30/12/98	AU 8052398 A	04/01/99
		SE 9702385 A	24/12/98
WO 9726731 A1	24/07/97	AU 2242697 A	11/08/97

Form PCT/ISA/210 (patent family annex) (July 1998)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification [6] : H04L 12/56, 29/02	A3	(11) International Publication Number: WO 98/59470 (43) International Publication Date: 30 December 1998 (30.12.98)

(21) International Application Number: PCT/SE98/01217

(22) International Filing Date: 23 June 1998 (23.06.98)

(30) Priority Data:
9702385-7 23 June 1997 (23.06.97) SE

(71) Applicants (*for all designated States except US*): TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE). TELIA AB [SE/SE]; S-123 86 Farsta (SE).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): KANTER, Theo [NL/SE]; Rönninge skolväg 35E, S-144 62 Rönninge (SE). FOGELHOLM, Rabbe [SE/SE]; Turraupen 54 B, S-191 47 Sollentuna (SE).

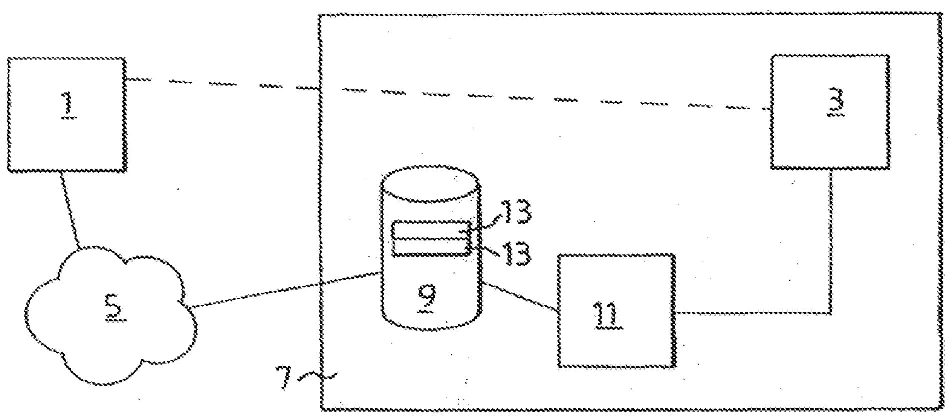
(74) Agents: HERBJØRNSEN, Rut et al.; Albihns Patentbyrå Stockholm AB, P.O. Box 3137, S-103 62 Stockholm (SE).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report: 18 March 1999 (18.03.99)

(54) Title: METHOD AND APPARATUS TO ENABLE A FIRST SUBSCRIBER IN A LARGER NETWORK TO RETRIEVE THE ADDRESS OF A SECOND SUBSCRIBER IN A VIRTUAL PRIVATE NETWORK



(57) Abstract

The present invention relates to an apparatus and a method for use in a virtual private network, VPN, (7, 7'), or a network domain forming part of a larger network, such as the Internet, to enable a first subscriber (1; 1') in the larger network to retrieve the address of a second subscriber (3; 3') in the VPN. The address may be returned to the first subscriber (1; 1') or a connection means (11) may set up the connection between the subscribers (1, 3; 1', 3') automatically.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/01217

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 12/56, H04L 29/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPIL, EDOC, JAPIO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ITU-T Recommendation H. 323, 1996, "Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service" Paragraph 6.4, 3.41, 3.43	4-6
Y		1-3,7-12
	--	
Y	IETF RFC 883, Volume, November 1983, P. Mockapetris, "DOMAIN NAMES - IMPLEMEntATION and SPECIFICATION" page 23	1-3,7-12
	--	
A	IETF RFC 1383, Volume, December 1992, C. Huitema, "An Experiment in DNS Based IP Routing", paragraph 2	1-12
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" erlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 January 1999	22 -01- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Christina Halldin Telephone No. + 46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/01217

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	IETF RFC 2052, Volume, October 1996, A. Gulbrandsen et al, "A DNS RR for specifying the location of services (DNS SRV)", see the whole document --	1-12
A	EP 0752674 A1 (SUN MICROSYSEMS, INC.), 8 January 1997 (08.01.97), abstract -- --------	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/12/98

International application No.

PCT/SE 98/01217

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0752674 A1	08/01/97	JP 9171465 A	30/06/97
		US 5745683 A	28/04/98

Form PCT/ISA/210 (patent family annex) (July 1992)

U 7388569

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 30, 2011

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF:

U.S. PATENT: *7,418,504*

ISSUE DATE: *August 26, 2008*

By Authority of the

Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office

T. Wallace

T. WALLACE

Certifying Officer

Plaintiffs' VirnetX Exhibit
VirnetX, Inc. v. Apple, Inc.
PX004
C.A. 6:10-cv-0417

VX00056852

US007418504B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.:** **US 7,418,504 B2**
(45) **Date of Patent:** **Aug. 26, 2008**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Scotts Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 646 days.

(21) Appl. No.: **10/714,849**

(22) Filed: **Nov. 18, 2003**

(65) **Prior Publication Data**

US 2004/0098485 A1 May 20, 2004

Related U.S. Application Data

(63) Continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/137,704, filed on Jun. 7, 1999, provisional application No. 60/106,261, filed on Oct. 30, 1998.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/226**

(58) **Field of Classification Search** 709/226, 709/221; 713/201
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846	A	6/1990	Humphrey et al.
4,988,990	A	1/1991	Warrior
5,164,988	A	11/1992	Matyas et al.
5,276,735	A	1/1994	Boebert et al.
5,311,593	A	5/1994	Carmi

(Continued)

FOREIGN PATENT DOCUMENTS

DE	199 24 575	12/1999

(Continued)

OTHER PUBLICATIONS

Laurie Wells (Lancasterbibelmail MSN Com); "Subject: Security Icon" Usenet Newsgroup, Oct. 19, 1998, XP002200606.

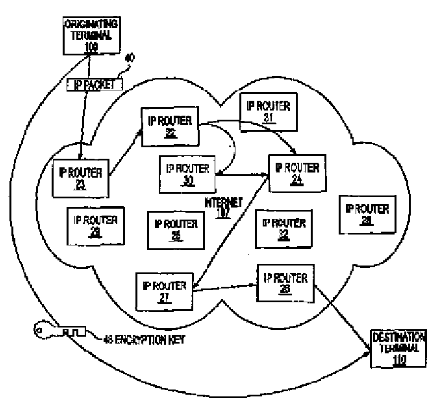
(Continued)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—McDermott Will & Emery, LLP

(57) **ABSTRACT**

A secure domain name service for a computer network is disclosed that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. The portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

60 Claims, 40 Drawing Sheets



U.S. PATENT DOCUMENTS

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.	
5,559,883	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	
5,654,695	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.	
5,774,660	A	6/1998	Brendel et al.	
5,787,172	A	7/1998	Arnold	
5,790,548	A	8/1998	Sistanizadeh et al.	
5,796,942	A	8/1998	Esbensen	
5,805,801	A	9/1998	Holloway et al.	
5,842,040	A	11/1998	Hughes et al.	
5,845,091	A	12/1998	Dunne et al.	
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, Jr. et al.	
5,905,859	A	5/1999	Holloway et al.	
5,918,019	A	6/1999	Valencia	
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, Jr. et al.	
6,055,574	A	4/2000	Smorodinsky et al.	
6,061,736	A	5/2000	Rochberger et al.	
6,079,020	A	6/2000	Liu	
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	
6,175,867	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.	
6,222,842	B1	4/2001	Sasyan 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.	
6,256,671	B1	7/2001	Strentzsch et al.	
6,263,445	B1	7/2001	Blumenau	
6,286,047	B1	9/2001	Ramanathan 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.	
6,324,161	B1	11/2001	Kirch	
6,330,562	B1	12/2001	Boden et al.	
6,332,158	B1	12/2001	Risley et al.	
6,353,614	B1	3/2002	Borella et al.	
6,425,003	B1	7/2002	Herzog 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	709/227
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.	
6,606,708	B1	8/2003	Devine 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	
6,714,970	B1	3/2004	Fiveash et al.	
6,717,949	B1	4/2004	Boden et al.	
6,751,738	B2	6/2004	Wesinger, Jr. 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.	
7,010,604	B1	3/2006	Munger et al.	
7,133,930	B2	11/2006	Munger et al.	
7,188,180	B2	3/2007	Larson et al.	
7,197,563	B2	3/2007	Sheymov et al.	
2002/0004898	A1	1/2002	Droge	
2003/0196122	A1	10/2003	Wesinger, Jr. et al.	
2005/0055306	A1	3/2005	Miller et al.	
2006/0059337	A1	3/2006	Polyhonen et al.	

FOREIGN PATENT DOCUMENTS

DE	199 24 575	A1	12/1999
EP	0 814 589		12/1997
EP	0 814 589	A	12/1997
EP	0 838 930		4/1998
EP	0 838 930	A	4/1998
EP	0 838 930	A2	4/1998
EP	836306	A1	4/1998
EP	0 858 189		8/1998
GB	2 317 792		4/1998
GB	2 317 792	A	4/1998
GB	2 334 181	A	8/1999
WO	9827783	A	6/1998
WO	WO 98/27783		6/1998
WO	WO 98 55930		12/1998
WO	WO 98 59470		12/1998
WO	WO 99 38081		7/1999
WO	WO 99 48303		9/1999
WO	WO 00/17775		3/2000
WO	WO 00/70458		11/2000
WO	WO 01 50688		7/2001

OTHER PUBLICATIONS

Davila J et al, "Implementatin of Virtual Private Networks at the Transport Layer", Information Security, Second International Workshop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-66695-B, retrieved from the Internet: URL: http://www.springerlink.com/content/4uac0tb0heccma89/fulltext.pdf>(Abstract).

Donald E. Eastlake, III, "Domain Name System Security Extensions", Internet Draft, Apr. 1998.

P. Srisuresh, et al., "DNS Extensions to Network Address Translators", Internet Draft, Jul. 1998.

D.B. Chapman, et al., "Building Internet Firewalls, chapters 8 and 10 (parts)", pp. 278-296 and pp. 351-375.

Search Report (dated Jun. 18, 2002), International Application No. PCT/US01/13260.

Search Report (dated Jun. 28, 2002), International Application No. PCT/US01/13261.

Donald E. Eastlake, "Domain Name System Security Extensions", DNS Security Working Group. Apr. 1998, 51 pages.

D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-297 and pp. 351-375.

P. Srisuresh et al., "DNS extensions to Network Address Translators", Jul. 1998, 27 pages.

Laurie Wells, "Security Icon", Oct. 19, 1998, 1 page.

W. Stallings, "Cryptography And Network Security", 2nd Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.