UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/019,519	**05/22/2024 03:21:37 PM Z ET**	**IVI785**

Title of Invention

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	7949785
CONFIRMATION #	2698	FILED BY	Ashley Cheung
PATENT CENTER #	65626750	FILING DATE	-
CUSTOMER #	23446	FIRST NAMED INVENTOR	Hasan S. Alkhatib
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Jordan Rossen

Documents

TOTAL DOCUMENTS: 19

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
EX1001_US7949785.pdf	47	Copy of patent for which reexamination is requested	4214 KB
EX1002_File History_10403818_Part1.pdf	126	Non Patent Literature	17452 KB
EX1002_File History_10403818_Part2.pdf	155	Non Patent Literature	16908 KB
EX1002_File History_10403818_Part3.pdf	255	Non Patent Literature	25000 KB
EX1002_File History_10403818_Part4.pdf	175	Non Patent Literature	17641 KB

EX1002_File History_10403818_Part5.pdf	124	Non Patent Literature	12736 KB
EX1004_Shamos_CV.pdf	74	Non Patent Literature	807 KB
EX1005_Leung_US7036143.pdf	21	Other reference-Patent/Application/Search Documents	2444 KB
EX1006_Forslow_US7155518.pdf	33	Other reference-Patent/Application/Search Documents	4211 KB
EX1007_Mehta_US20030028671A1.pdf	24	Other reference-Patent/Application/Search Documents	3310 KB
EX1008_Kong_US7290060.pdf	14	Other reference-Patent/Application/Search Documents	1728 KB
EX1009_Volz_US7533164.pdf	38	Other reference-Patent/Application/Search Documents	3664 KB
EX1010_DistrictCourtInfringementChart.pdf	20	Non Patent Literature	1093 KB
IDS_IVI785.pdf	2	Reexam - Info Disclosure Statement Filed by 3rd Party	147 KB
Exhibit_AA_785_CC.pdf	29	Non Patent Literature	2572 KB
EX1003_Declaration_M_Shamos.pdf	26	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	2744 KB
COS_IVI785.pdf	2	Reexam Certificate of Service	93 KB
Transmittal_IVI785.pdf	5	Transmittal Letter	262 KB

Request_IVI785.pdf	27	Receipt of Original Ex Parte Request by Third Party	918 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
EX1001_US7949785.pdf	D2FC33DC6EDF3F39211DBFD06AE6E1E3FBCE48FDE8BCFFB757CF5D0CE961F8E54BDF58C41210A4759B21F3111257914E61B68D21A35E6D4E9010B92408808B73
EX1002_File History_10403818_Part1.pdf	8DF9C4215F054498B6BC2856BFB043C0C8C74BC3CC60E89B12589C16B58D69A84AEF364B2524D13F590FFBC95DA6C8A99769D87D7B5465C56648BDED21D28672
EX1002_File History_10403818_Part2.pdf	EC47952F116BE916FEDE3E7CB64577F8BC9C261DBF82265C5B5F3221DD540050F6E3906CA847516CE64810368AE4B925C6F728A3A89884177BC81E4EBDFFB080
EX1002_File History_10403818_Part3.pdf	B4D5DB67393B180969AFE7DC365E7C9F33A88FEE8F9597F5136F010606FA7CFD7D25E90418F2A8406818FBF2D30899396EBF7D8CFFF164D2004159A869F3D5E5
EX1002_File History_10403818_Part4.pdf	B50C2A2BF838490BA497967388748C98A4F234DA84A0BA3EAEF42F411B5DCFF69938D502DEC42ACD646BA719FDEE227AF2E19AE5E8C007DE46A99D90F9A023C7
EX1002_File History_10403818_Part5.pdf	2B484BCF0593410603E213EC782C9152FEC01F6E05B5B6ABFE1FC6AE4D70A0C2963DC7D27B30BF49DFD107A0C8D8364E7740713AEE5C9E85AA1084E30A55351F
EX1004_Shamos_CV.pdf	181ED2CE3A6ABB834077C8115FFE36CA156B88FF3B23A4983467ACD84C18AC813ED781399F7F0177870B7CFC523D7C93E2FBD008F91AA201F3AB8B387DCB38ED
EX1005_Leung_US7036143.pdf	FAA474A91FBBEC7371B52615B8362A411791B1069CF01BB341274CAF42A841283E80612E874A712C8DB300136AD3203A59378E475E345815BB2733028B22BB6F

EX1006_Forslow_US7155518.pdf	F6B8E43BC469AFB422F70099199F8D569D0013CAF239829A8C6185C6AB4F8B28645CAE18FA7A4CF2218754EDAE6DAEB0744F12BA09D38F00C6B416D57F344E64
EX1007_Mehta_US20030028671A1.pdf	228990CCC783C50E0D63CCB9764F9559DF54F3D68BDE4583B5A9FD7B28392D96952D729869679563CA3DA465A4137ADBFDDA83E025505D593C96C7478A493913
EX1008_Kong_US7290060.pdf	EF774BEF8E7F77CE593694E10C649E7F287C244C072F5BDB091B39B5E63980FC4F24450D95ACEEFEDC93382082E6F0164A0044BFD1D5A93DA320E6FEE9D049A2
EX1009_Volz_US7533164.pdf	7A4F06E5E838B05E4C3A01CD62816D54638E1118A77DEDDEDF93E8DCF32ED4B269BA2033FBED0081E1358E9DD7F14E813A94F5A61DC22B873280A5910D6874E7
EX1010_DistrictCourtInfringementChart.pdf	43455CDD4F67E21F03C7DE32CF9188CB305E8CCE64F2FF6D4B5AF8FE7AE2D646E9DD62980FAB0753C75D6EFA2A373A1531C5C5BDBA5B9B3829E57DCEE953EF0E
IDS_IVI785.pdf	C9F17E84E17A82EBB95D5AA42978EF0D21C3842B504DED755F8C4461FDE1A921BE7F389FEEB966FE7ADCE042C02B272CF5BF0BF55712E47AC9EFEE60AF39D277
Exhibit_AA_785_CC.pdf	CE5B7A6067302E9E8F3B6C49FE1C6D8233B7692967453873A3031DBE702167502BB24F3947802D4C46A1ABC742C4DE1E08E2C2C8A311E1FC9F2D00447DEBA233
EX1003_Declaration_M_Shamos.pdf	96DF3AF0E206B043D8BE9B1BBF350BED60E432E6095380BC4DA25D35184A841F2E12203B50ADD15FE061D07E82474EBBCFB0BD686225EED08F40BE4E4C5654BA
COS_IVI785.pdf	BFF5A19397DA84EAC69D6F24ED181C23B1B97846B537A42F055717422FC6BDC2825ED9FA4A0C350E08DA5BE8259B060FE66380A83B3DF435CD14F8334E73579E
Transmittal_IVI785.pdf	718FCC059C0DA75B13941A6CA20CEFD8DD6DAF1D1A9EBF13E06988B876785717FDB7A560C7AEAE40844ACD897B4B8C8DAFDF95697100F6DA9BBA7E7BFAE5A066

Request_JVI785.pdf 0716BE24B36171E5F305B3A5A09B69AC5CBF381FD9A6ED83D7A506E80F9E9D1C04258C3FBEB90E906089D38B3DB74C90DF7335A431D43F16BC432D208FAAA185

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/019,519	05/22/2024 03:21:37 PM Z ET	IVI785

Title of Invention

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	7949785
CONFIRMATION #	2698	FILED BY	Ashley Cheung
PATENT CENTER #	65626750	AUTHORIZED BY	Jordan Rossen
CUSTOMER #	23446	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Hasan S. Alkhatib

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
DA / 506990	E20245LF23068350	Ashley Cheung

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1812	REQUEST FOR EX PARTE REEXAM-NON-STREAMLINED	12600.00	1	12600.00
			TOTAL AMOUNT:	$12,600.00

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 filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

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

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C.

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

New International Application Filed with the USPTO as a Receiving Office

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

EXHIBIT 1009

U.S. Patent No. 7,533,164 to *Volz et al.*

("*Volz*")

US007533164B2

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

(10) **Patent No.: US 7,533,164 B2**
(45) **Date of Patent: May 12, 2009**

(54) **METHOD AND SYSTEM FOR ENABLING CONNECTIONS INTO NETWORKS WITH LOCAL ADDRESS REALMS**

(75) Inventors: **Bernie Volz**, Center Harbor, NH (US); **George Chambert**, Uppsala (SE); **Martin Korling**, Sollentuna (SE); **Bjorn Landfeldt**, Menai (AU); **Yuri Ismailov**, Kista (SE)

(73) Assignee: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 29 days.

(21) Appl. No.: **10/510,546**

(22) PCT Filed: **Mar. 28, 2003**

(86) PCT No.: **PCT/US03/09834**

§ 371 (c)(1),
(2), (4) Date: **Apr. 25, 2005**

(87) PCT Pub. No.: **WO03/088625**

PCT Pub. Date: **Oct. 23, 2003**

(65) **Prior Publication Data**

US 2005/0223095 A1 Oct. 6, 2005

Related U.S. Application Data

(60) Provisional application No. 60/370,812, filed on Apr. 8, 2002.

(51) **Int. Cl.**
G06F 15/16 (2006.01)
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/223**; 709/245

(58) **Field of Classification Search** 709/223, 709/220, 226, 227, 238, 230, 244, 245, 250
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,886,103 B1 * 4/2005 Brustoloni et al. 726/15

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0817444 A 1/1998

(Continued)

OTHER PUBLICATIONS

Srisuresh P et al., "RFC 2694; DNS Extensions to Network Address Translators (DNS ALG)", Sep. 1999, Internet Engineering Task Force XP002247781.

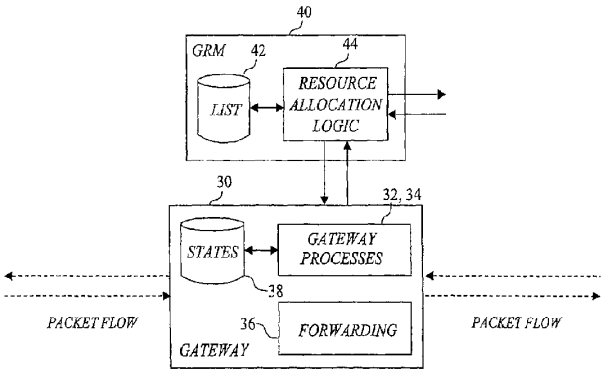
(Continued)

Primary Examiner Jeffrey Pwu
Assistant Examiner—Benjamin R Bruckart
(74) *Attorney, Agent, or Firm*—Nixon & Vanderhye P.C.

(57) **ABSTRACT**

The invention generally concerns the issue of providing connectivity between two different address realms, generally referred to as an inside realm and an outside realm, by establishing connections through an intermediate gateway. The gateway normally has a number of outside-realm gateway addresses for enabling representation of inside-realm nodes in the outside realm. In a first aspect, support for flexible outside-realm initiated connections is enabled by dynamically establishing new gateway connection states triggered, for each new connection, by a respective user-resource identifier query initiated from a corresponding outside node. In a second aspect of the invention, intelligent use of predetermined connection information in the process of setting up new gateway connection states makes it possible to significantly increase the number of connections that can be simultaneously supported by the gateway using a limited number of outside-realm addresses.

60 Claims, 15 Drawing Sheets



U.S. PATENT DOCUMENTS

6,892,245 B1 * 5/2005 Crump et al. 709/245

FOREIGN PATENT DOCUMENTS

WO WO 9930467 A 6/1999

OTHER PUBLICATIONS

Srisuresh P et al., "Middlebox communication architecture and framwork", Internet Engineering Task Force, XX.XX, Feb. 28, 2002.

C Huitema, "Midcom Scenarios; draft-ietf-midcom-scenarios-02.txt>", May 17, 2001, Internet Engineering Task Force, Internet XP002247782.

Dias D M et al., "A scalable and highly available web server" Digest of Papers of Compcon (Computer Society Conference) 1996 Technologies for the Information Superhighway. Santa Clara, Feb. 25-28, 1996, Digest of Papers of the Computer Society Computer Conference Compcon, Los Alamitos, IEEE Comp. Soc. Press, vol. Conf. 41, Feb. 25, 1996, pp. 85-92, XP010160879, ISBN: 0-8186-7414-8, the whole document.

European Patent Office, International Search Report for PCT/US03/09834, dated Jul. 21, 2003.

P. Srisuresh et al., IP Network Address Translator (NAT) Terminology and Considerations. Network Working Group, Request for Comments: 2663, Aug. 1999, pp. 1-27.

M. Borella et al., Realm Specific IP: Framework, Network Working Group, Request for Comments: 3102, Oct. 2001, pp. 1-27.

M. Borella et al., Real Specific IP: Protocol Specification, Network Working Group. Request for Comments: 3103, Oct. 2001, pp. 1-.

Y. Rekhter et al., Address Allocation for Private Internets, Network Working Group. Request for comments: 1918. Feb. 1996, pp. 1-9.

M. Handley, SIP: Session Initiation Protocol, Network Working Group, Request for Comments: 2543, Mar. 1999, pp. 1-135.

e-Boarder Solution Series 1: Solving NAT and Private IP Problems, Permeo Technologies, Inc., Jul. 2001, pp. 1-8.

* cited by examiner

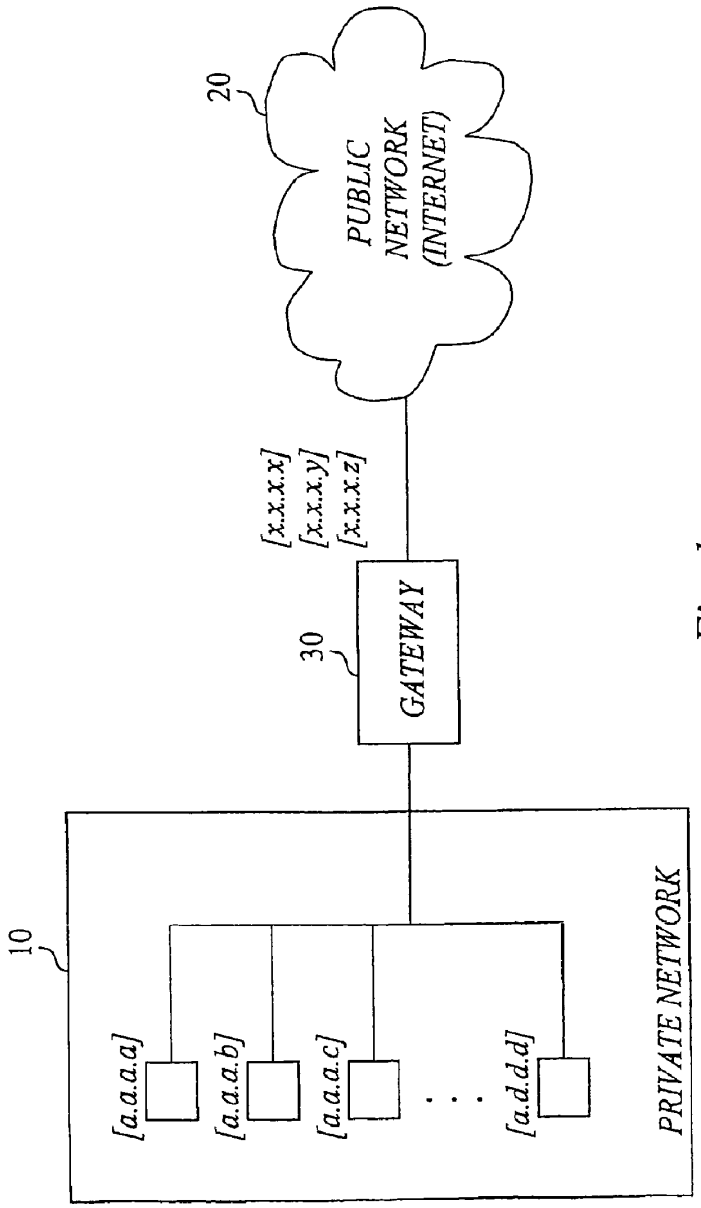


Fig. 1
(Prior art)

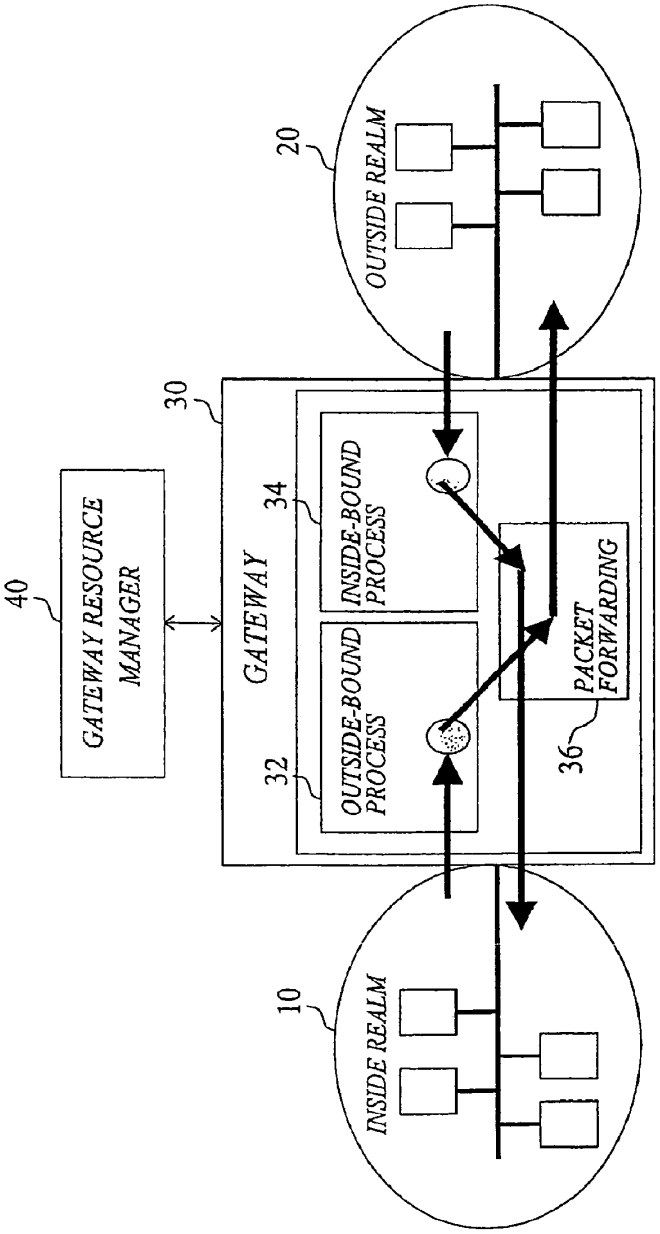


Fig. 2

AA/SWA Ex. 1015, p.12 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

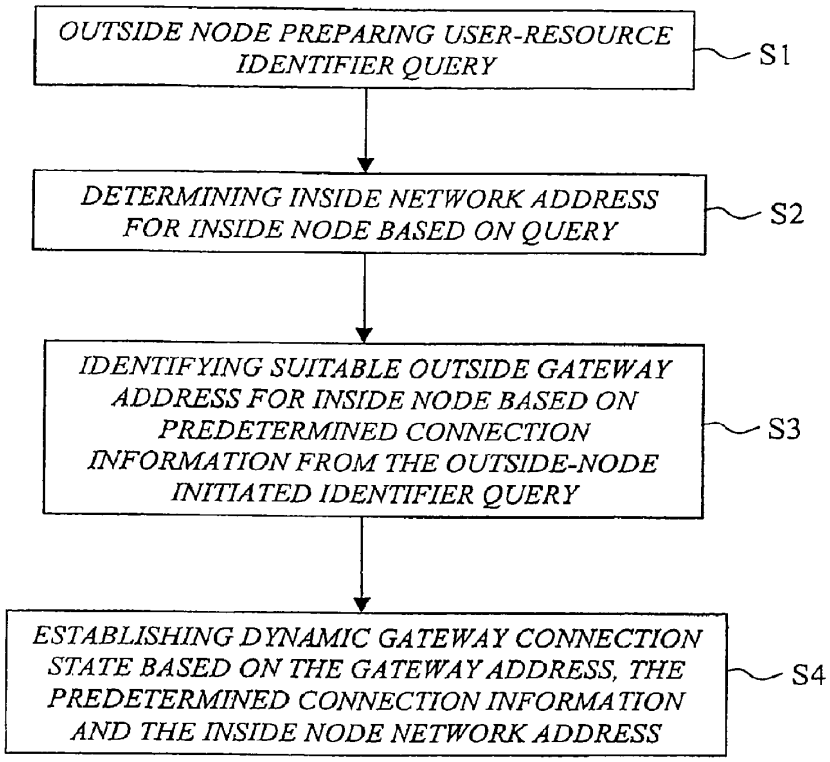

OUTSIDE NODE PREPARING USER-RESOURCE IDENTIFIER QUERY
S1
DETERMINING INSIDE NETWORK ADDRESS FOR INSIDE NODE BASED ON QUERY
S2
IDENTIFYING SUITABLE OUTSIDE GATEWAY ADDRESS FOR INSIDE NODE BASED ON PREDETERMINED CONNECTION INFORMATION FROM THE OUTSIDE-NODE INITIATED IDENTIFIER QUERY
S3
ESTABLISHING DYNAMIC GATEWAY CONNECTION STATE BASED ON THE GATEWAY ADDRESS, THE PREDETERMINED CONNECTION INFORMATION AND THE INSIDE NODE NETWORK ADDRESS
S4

Fig. 3

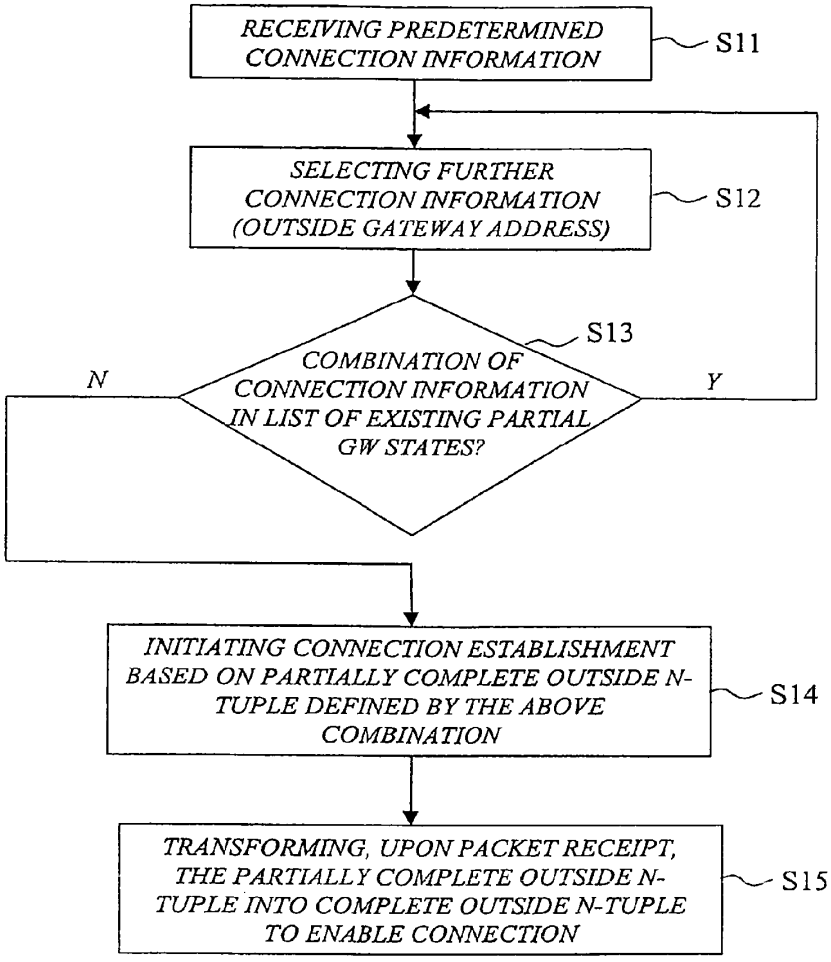

RECEIVING PREDETERMINED CONNECTION INFORMATION
S11
SELECTING FURTHER CONNECTION INFORMATION (OUTSIDE GATEWAY ADDRESS)
S12
S13
COMBINATION OF CONNECTION INFORMATION IN LIST OF EXISTING PARTIAL GW STATES?
N
Y
INITIATING CONNECTION ESTABLISHMENT BASED ON PARTIALLY COMPLETE OUTSIDE N-TUPLE DEFINED BY THE ABOVE COMBINATION
S14
TRANSFORMING, UPON PACKET RECEIPT, THE PARTIALLY COMPLETE OUTSIDE N-TUPLE INTO COMPLETE OUTSIDE N-TUPLE TO ENABLE CONNECTION
S15

Fig. 4

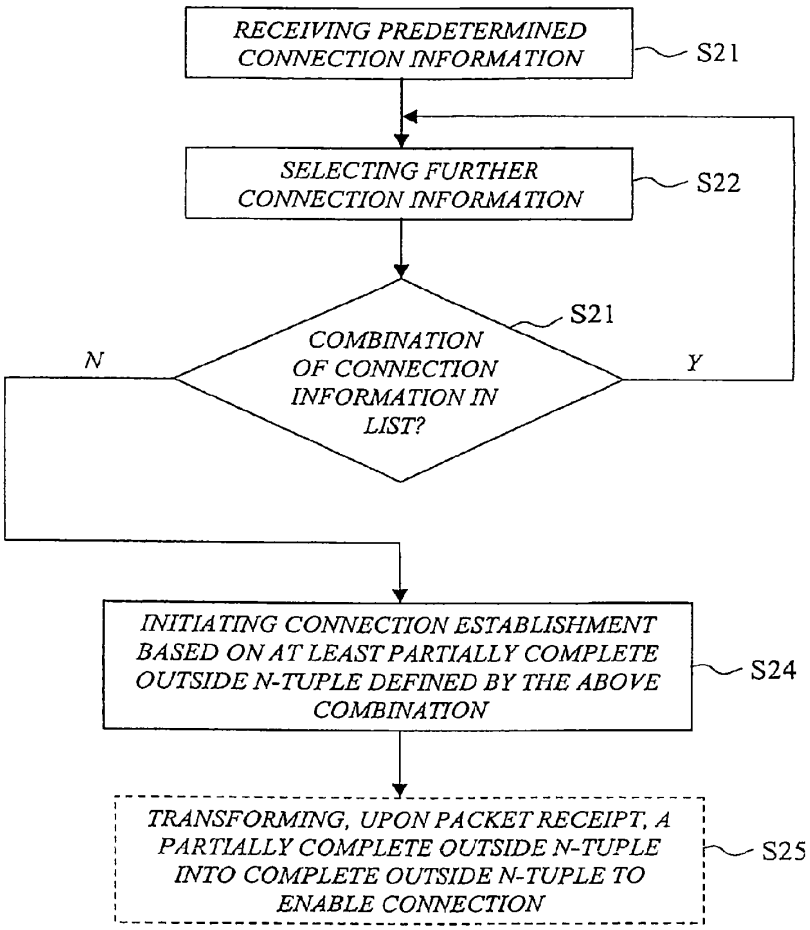

RECEIVING PREDETERMINED CONNECTION INFORMATION
S21
SELECTING FURTHER CONNECTION INFORMATION
S22
COMBINATION OF CONNECTION INFORMATION IN LIST?
S21
N
Y
INITIATING CONNECTION ESTABLISHMENT BASED ON AT LEAST PARTIALLY COMPLETE OUTSIDE N-TUPLE DEFINED BY THE ABOVE COMBINATION
S24
TRANSFORMING, UPON PACKET RECEIPT, A PARTIALLY COMPLETE OUTSIDE N-TUPLE INTO COMPLETE OUTSIDE N-TUPLE TO ENABLE CONNECTION
S25

Fig. 5

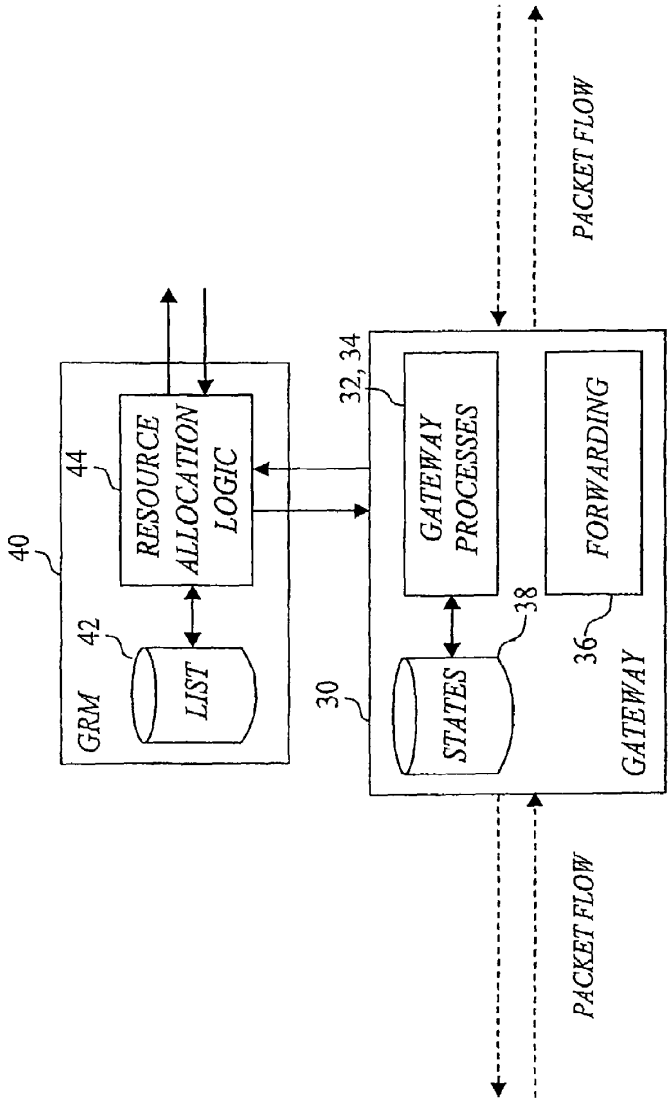

PACKET FLOW
32, 34
GATEWAY PROCESSES
FORWARDING
RESOURCE ALLOCATION LOGIC
44
40
42
LIST
GRM
30
STATES
38
36
GATEWAY
PACKET FLOW

Fig. 6

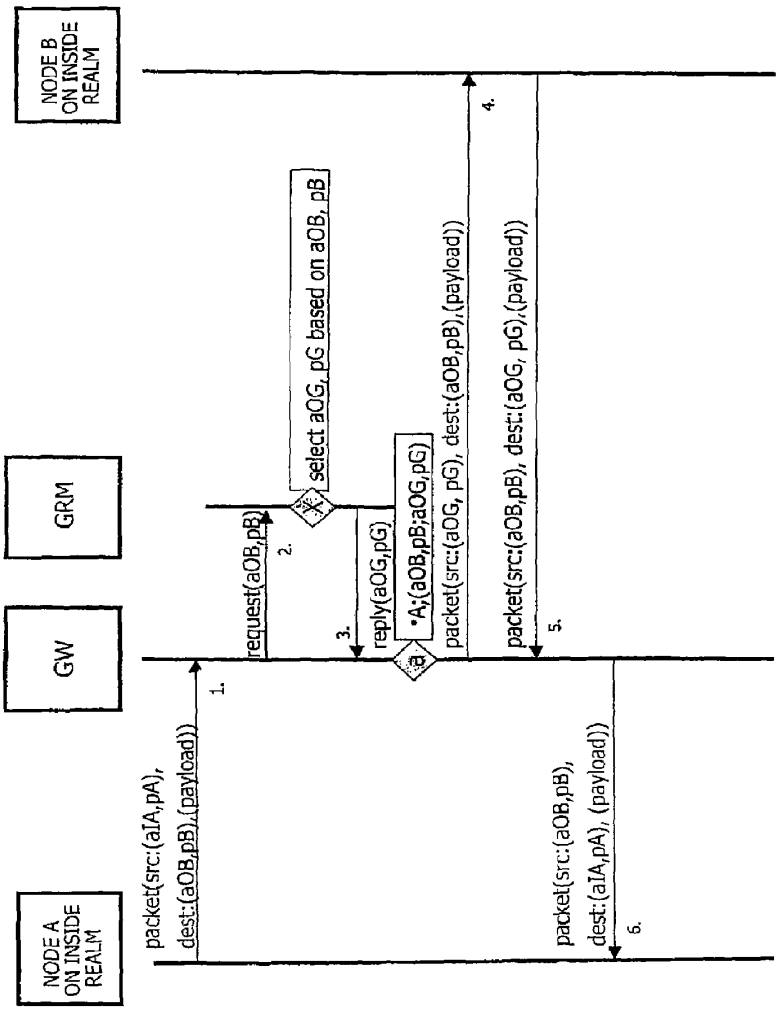


Fig. 7

AA/SWA Ex. 1015, p.17 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

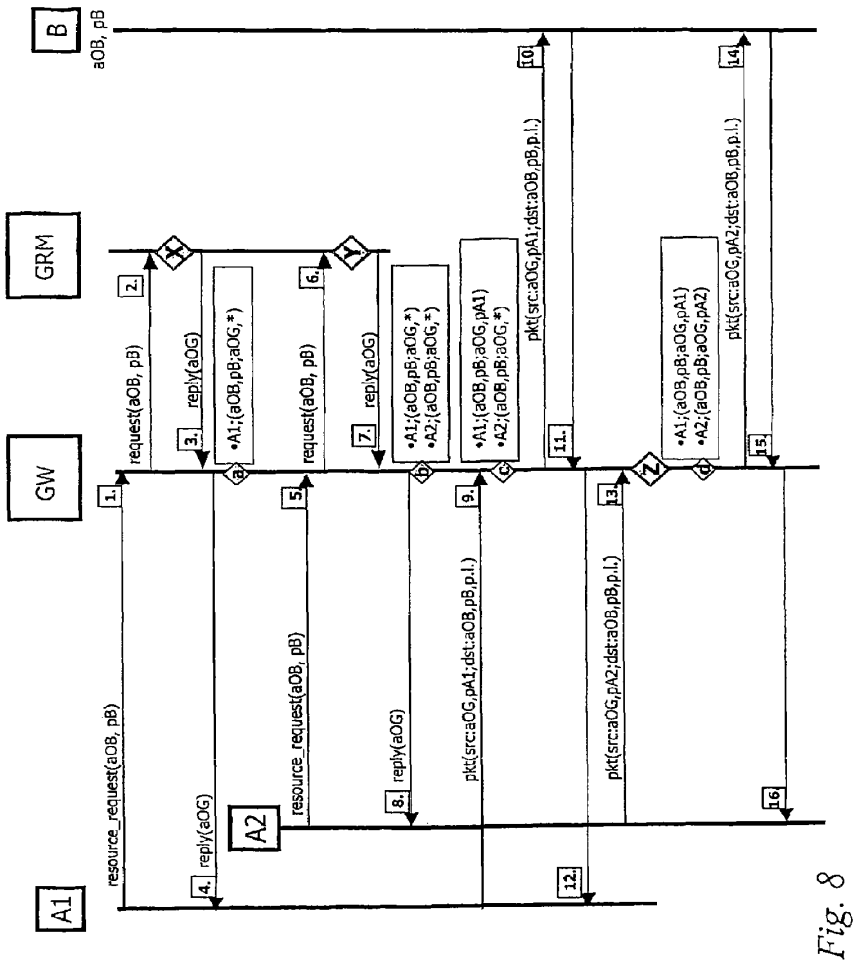

B
aOB, pB
GRM
GW
A1
A2
request(aOB, pB)
reply(aOG)
•A1:{aOB,pB;aOG,*)
resource_request(aOB, pB)
•A2:{aOB,pB;aOG,*)
pkt(src:aOG,pA1;dst:aOB,pB,p.l.)
pkt(src:aOG,pA2;dst:aOB,pB,p.l.)
X
Y
Z
a
b
c
d

Fig. 8

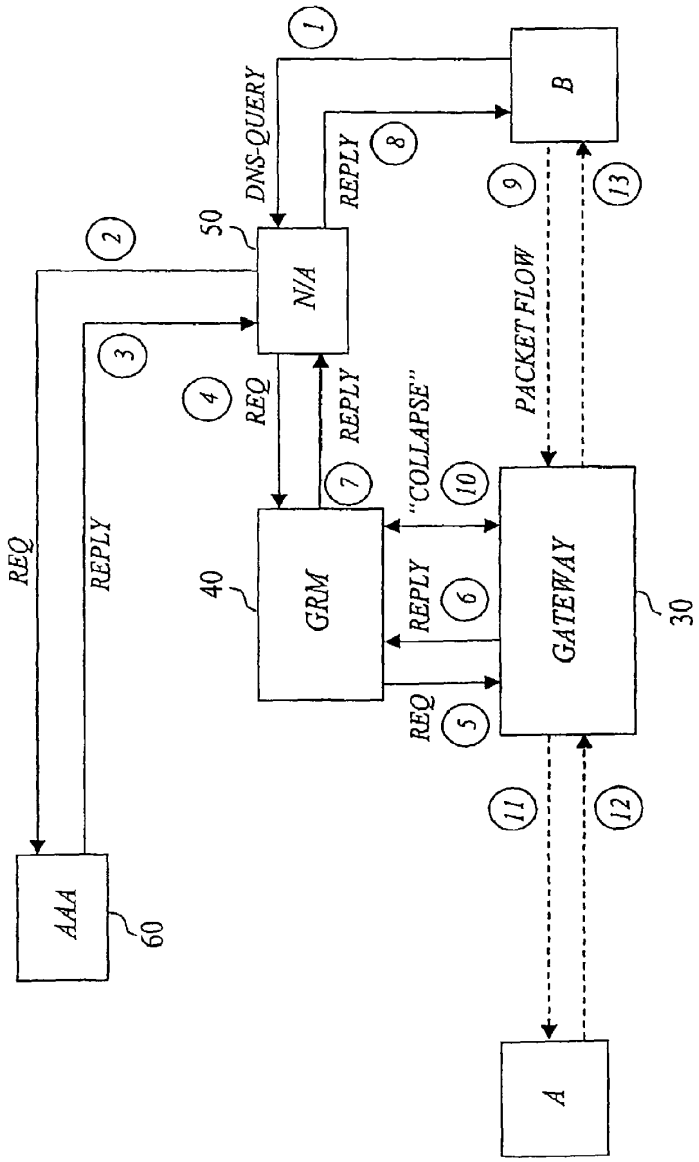


Fig. 9

AA/SWA Ex. 1015, p.19 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

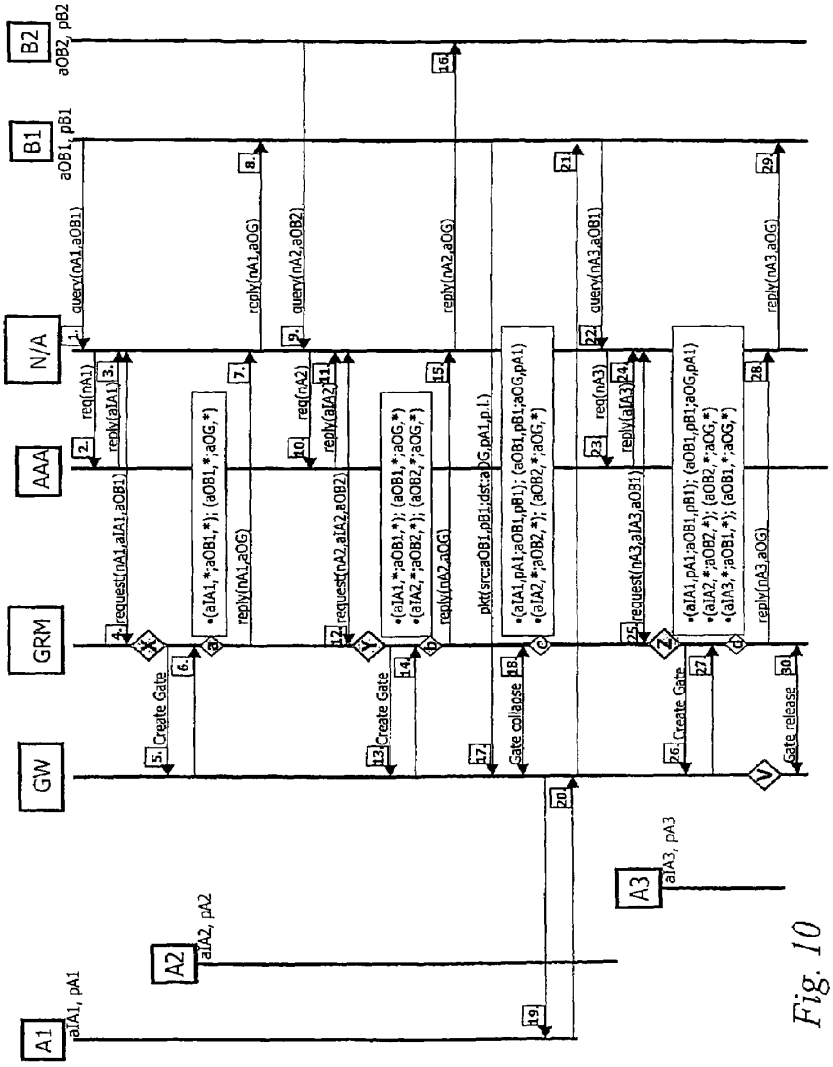

B2
aOB2, pB2
B1
aOB1, pB1
N/A
AAA
GRM
GW
A1
aIA1, pA1
A2
aIA2, pA2
A3
aIA3, pA3
query(nA1,aOB1)
reply(nA1,aOG)
query(nA2,aOB2)
reply(nA2,aOG)
query(nA3,aOB1)
reply(nA3,aOG)
req(nA1)
reply(aIA1)
req(nA2)
reply(aIA2)
req(nA3)
reply(aIA3)
request(nA1,aIA1,aOB1)
reply(nA1,aOG)
request(nA2,aIA2,aOB2)
reply(nA2,aOG)
pkt(srcaOB1,pB1;dst:aOG,pA1,p1)
request(nA3,aIA3,aOB1)
reply(nA3,aOG)
Create Gate
Gate collapse
Gate release
X
Y
Z
a
b
c
d

Fig. 10

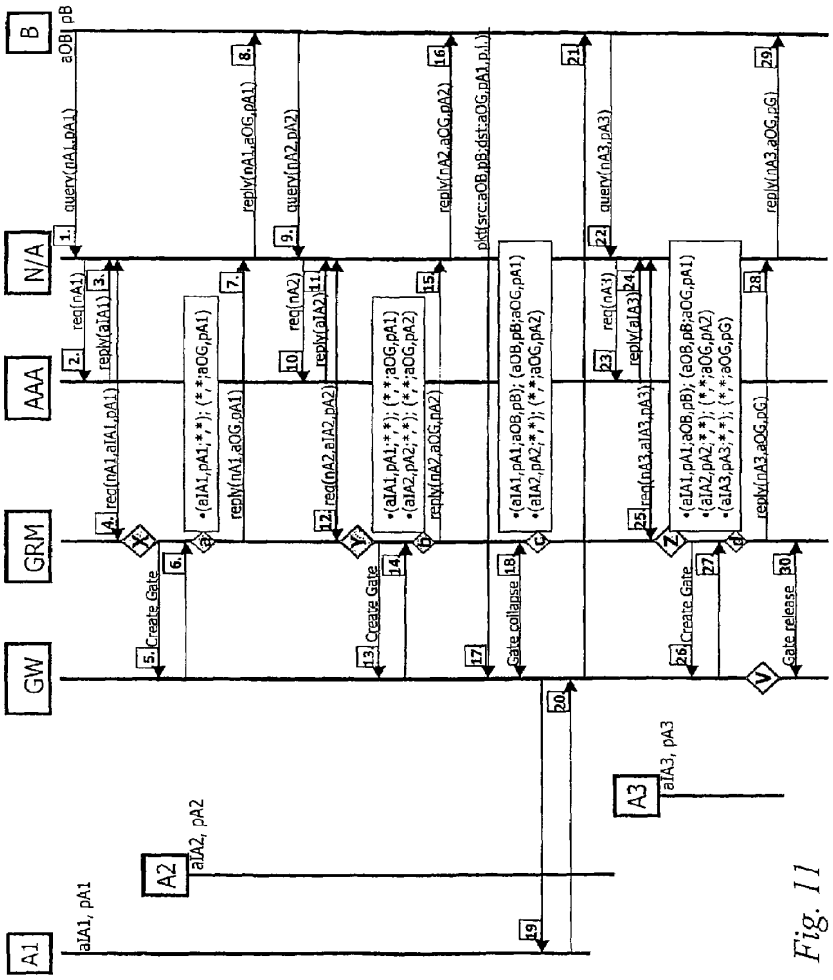

B
N/A
AAA
GRM
GW
A1
A2
A3
aOB, pB
query(nA1,pA1)
reply(nA1,aOG,pA1)
query(nA2,pA2)
reply(nA2,aOG,pA2)
pkt(src:aOB,pB;dst:aOG,pA1,pL)
query(nA3,pA3)
reply(nA3,aOG,pG)
req(nA1)
reply(aIA1)
req(nA2)
reply(aIA2)
req(nA3)
reply(aIA3)
req(nA1,aIA1,pA1)
reply(nA1,aOG,pA1)
req(nA2,aIA2,pA2)
reply(nA2,aOG,pA2)
req(nA3,aIA3,pA3)
reply(nA3,aOG,pG)
Create Gate
Create Gate
Gate collapse
Create Gate
Gate release
aIA1, pA1
aIA2, pA2
aIA3, pA3

Fig. 11

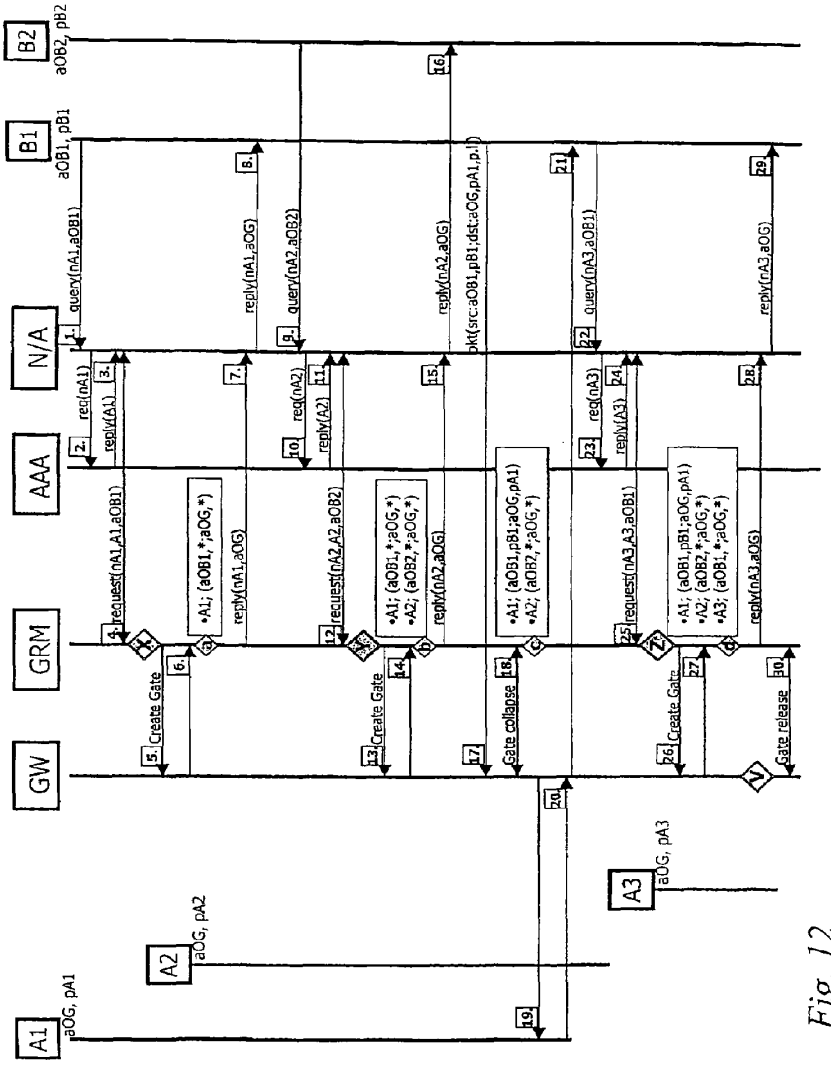

B2
aOB2, pB2
B1
aOB1, pB1
N/A
AAA
GRM
GW
A1
aOG, pA1
A2
aOG, pA2
A3
aOG, pA3
query(nA1,aOB1)
reply(nA1,aOG)
query(nA2,aOB2)
reply(nA2,aOG)
pkt(src:aOB1,pB1;dst:aOG,pA1,p.l)
query(nA3,aOB1)
reply(nA3,aOG)
req(nA1)
reply(A1)
req(nA2)
reply(A2)
req(nA3)
reply(A3)
request(nA1,A1,aOB1)
reply(nA1,aOG)
request(nA2,A2,aOB2)
reply(nA2,aOG)
request(nA3,A3,aOB1)
reply(nA3,aOG)
Create Gate
Create Gate
Gate collapse
Create Gate
Gate release

Fig. 12

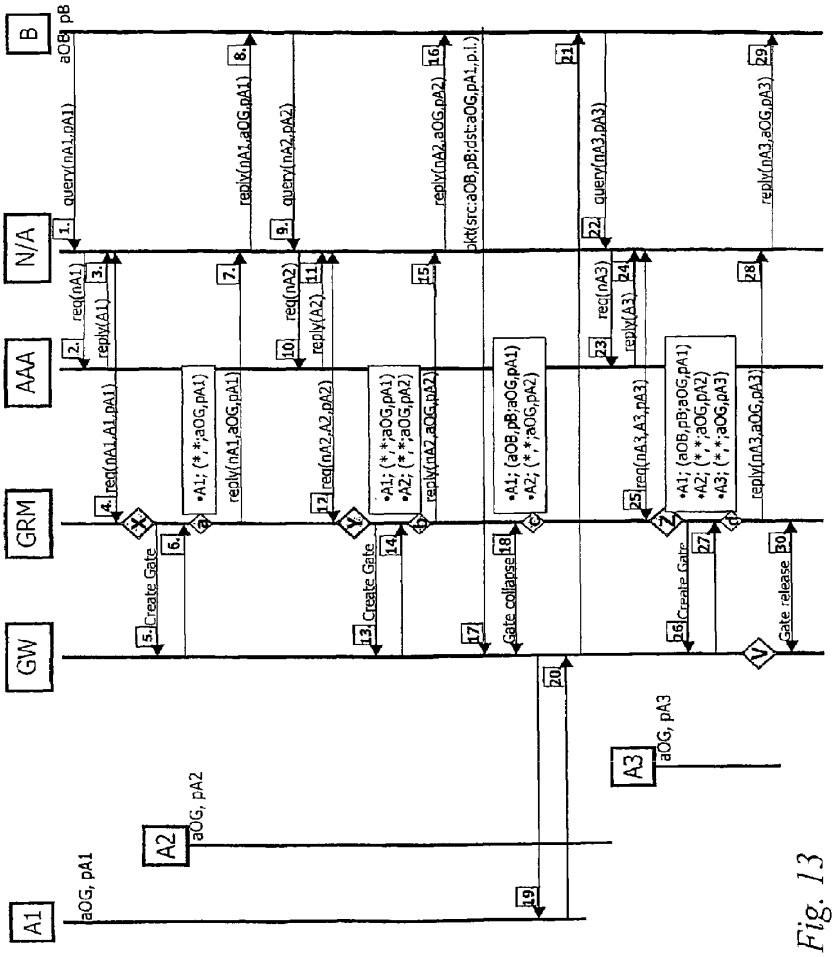

B
N/A
AAA
GRM
GW
A1
A2
A3
aOB, pB
query(nA1,pA1)
reply(nA1,aOG,pA1)
query(nA2,pA2)
reply(nA2,aOG,pA2)
pkt(src:aOB,pB;dst:aOG,pA1,p.l.)
query(nA3,pA3)
reply(nA3,aOG,pA3)
req(nA1)
reply(A1)
req(nA2)
reply(A2)
req(nA3)
reply(A3)
req(nA1,A1,pA1)
reply(nA1,aOG,pA1)
req(nA2,A2,pA2)
reply(nA2,aOG,pA2)
req(nA3,A3,pA3)
reply(nA3,aOG,pA3)
•A1; (*,*;aOG,pA1)
•A2; (*,*;aOG,pA2)
•A3; (*,*;aOG,pA3)
•A1; (aOB,pB;aOG,pA1)
•A2; (*,*;aOG,pA2)
•A3; (*,*;aOG,pA3)
Create Gate
Gate collapse
Gate release
aOG, pA1
aOG, pA2
aOG, pA3

Fig. 13

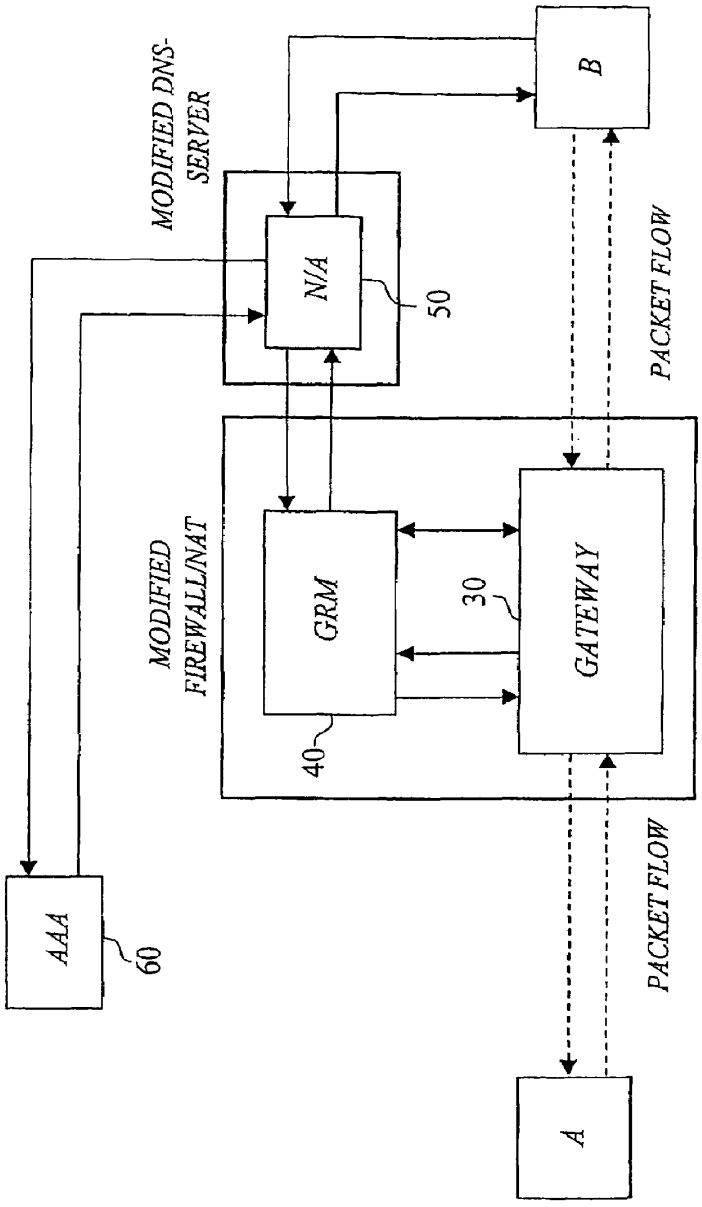


Fig. 14

AA/SWA Ex. 1015, p.24 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

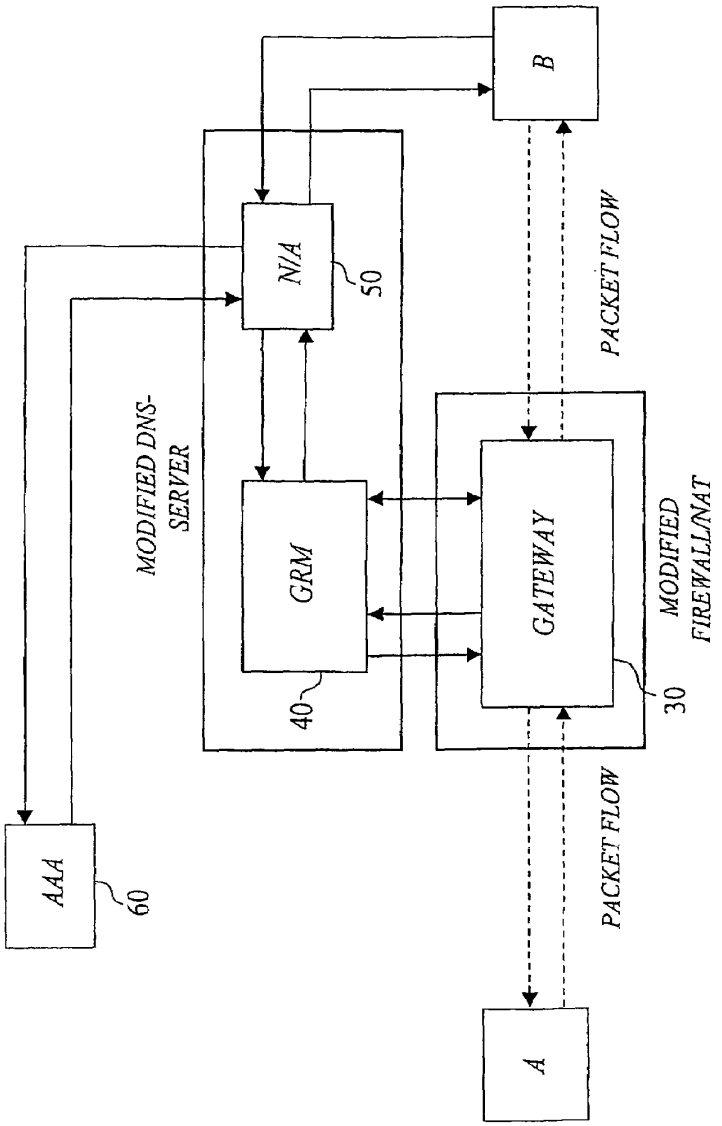

B
N/A
50
PACKET FLOW
MODIFIED DNS-SERVER
GRM
GATEWAY
MODIFIED FIREWALL/NAT
40
30
AAA
60
PACKET FLOW
A

Fig. 15

METHOD AND SYSTEM FOR ENABLING CONNECTIONS INTO NETWORKS WITH LOCAL ADDRESS REALMS

This application claims the benefit of U.S. provisional patent application Ser. No. 60/370,812, filed Apr. 8, 2002.

TECHNICAL FIELD OF THE INVENTION

The present invention generally relates to network communication and more particularly to the issue of providing connectivity between networks of different address realms.

BACKGROUND OF THE INVENTION

In network communication, there is a general demand for providing connectivity between different networks, especially when the networks have different address realms. For example, this would normally be the case when a node in a private network wants to connect to a host in a public network. The private network usually have internal addresses that cannot be used outside the network, for privacy reasons or simply because the internal addresses are invalid for use outside the network. Other examples include connectivity between networks of different public domains, as well as between different private networks.

With the explosive growth of Internet Protocol (IP) networks such as the Internet, intranets and other networks, the limited IP address space offered by the current version of the IP protocol, IPv4, becomes a real challenge. With a 32-bit address field, it is possible to assign 2^{32} different addresses, which are about 4 billion globally unique addresses. The next version of the IP protocol, IPv6, will have a 128-bit address field, thus providing a virtually unlimited number of globally unique IP addresses. The challenge is that there is a limited number of IPv4 addresses available to the operators for their new networks, and IPv6 is not yet supported by more than a very limited set of nodes within the Internet. Also, a large number of legacy networks including Internet subnets will likely be using the IPv4 or older versions of the IP protocol for many years to come.

For mobile or cellular networks, telecom vendors and operators are facing a great challenge deploying support for an expected vast number of IP-enabled mobile terminals in 2.5 and 3G networks. The IPv4 address space is apparently not large enough to cover the needs when a massive deployment of 2.5 and 3G networks takes place within the near future. Today, network operators that apply for address ranges for their new cellular networks receive address spaces far below the expected number of users. The ratio can be as low as a few thousand addresses for an expected customer base of millions of subscribers.

To meet the demand for addresses, telecom vendors are pushing the introduction of IPv6 into terminals as the standard protocol to use within next generation cellular networks. IPv6, fully deployed would naturally solve the address space problem, but unfortunately, IPv6 is not widely deployed in the Internet yet, and it is expected that this deployment will be quite slow, at least in the near future. Since IPv6 is not deployed in the Internet, vendors will have to use migration schemes for providing connectivity between different networks.

There are a number of existing schemes for both extending an address realm and for translating between different address realms. These schemes will be briefly outlined below, mainly with respect to the issue of providing connectivity between private and public networks operating under the IP protocol.

With reference to FIG. **1**, a private realm is a domain where hosts are assigned addresses that are not unique within the Internet, or they are unique but for some reason they are hidden from the public realm. A common example is to assign hosts in a private network **10** with private addresses [a.a.a.a] to [a.d.d.d], for example as specified in RFC1918, to enable multiple hosts to share a single or some public IP addresses when the number of private realm hosts exceeds the number of public addresses assigned for the private network **10**. Since there is no assigned body coordinating the use of private addresses, these addresses occur at multiple locations around the world and therefore they are generally not unique and can thus not be used within the public realm. In order for private hosts to be able to access the public realm network **20**, a gateway **30** can be used for enabling multiple private hosts to share a single or some public IP addresses [x.x.x.x] to [x.x.x.z] for the purpose of public realm access. The gateway **30** thus provides the necessary means for connecting hosts within the private realm to the public realm, especially when the number of private hosts is larger than the number of available public IP addresses.

Network Address Translator (NAT)

Existing schemes for extending address realms such as the IPv4 address space are often based on so-called Network Address Translator (NAT) gateways, which translate private addresses into public addresses and vice versa [1]. The different flavors of NAT have in common that they all hide private addresses and reuse public addresses to enable communication between hosts in a private realm and hosts in the public realm.

Traditional NAT

A traditional NAT gateway typically uses a set of public IP addresses to assign to individual private nodes on a per-session basis. When a host within the private realm wants to contact a host within a public network such as the Internet, the NAT assigns one of its public addresses [x.x.x.x] to [x.x.x.z] to the private host. The NAT then rewrites the sender address in the IP header of the outgoing packet with the public address so the corresponding host in the public Internet gets the impression that the packet came from the publicly assigned IP address. When the public host sends a packet back to the publicly assigned address, the NAT rewrites the destination address in the IP header with the private address so the packet is correctly routed in the private realm.

This method of translating between the two realms is simple but suffers from two drawbacks other methods have tried to solve. Firstly, it does not allow a host in the public Internet to connect to a host within the private realm and secondly, it does not scale very well since every time a private host wants to connect to a public realm host, an entire public IP address is reserved for the host.

Network Address Port Translation (NAPT)

NAPT alleviates the scalability problem by enabling multiple private realm hosts to share a single IP address. This is accomplished by including transport protocol port information into the translation procedure. When a host in the private realm wants to connect to a host in the public realm, the gateway assigns a free port on the public realm interface to the connection and uses the original and assigned ports together with the IP addresses for the translation. This way the NAPT gateway can share a single IP address among several private hosts.

For example, consider a host [a.a.a.a] that wants to connect to host [d.d.d.d] on the public Internet. When the first packet to host [d.d.d.d] reaches the NAT it assigns a free port on an

AA/SWA Ex. 1015, p.26 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

interface, say public IP address [x.x.x.x], to the connection and rewrites the sender address from [a.a.a.a] into [x.x.x.x] and the sender port number to the assigned port number. When the receiver replies the destination address is [x.x.x.x] and the port is the assigned port number. When this packet reaches the NAPT gateway, it rewrites the destination address with [a.a.a.a] and the destination port number with the original port number.

Thus, NAPT scales better than traditional NAT, but it is still impossible for hosts within the public realm to initiate sessions to hosts within the private realm.

Bi-directional NAT

Bi-directional NAT enables hosts on the public Internet to reach hosts within a private realm. This is accomplished through the introduction of a special Application Layer Gateway (ALG), to a Domain Name Server (DNS) in conjunction with the bi-directional NAT. The ALG is capable of resolving Fully Qualified Domain Names (FQDN) of private realm hosts to assigned public realm addresses. The ALG is capable of translating the private realm address corresponding to a FQDN into a public realm address and vice versa. The bi-directional NAT allows hosts within the public Internet to communicate with hosts within a private realm, but there is a one-to-one mapping between hosts and public IP addresses which scales poorly when public IP addresses are scarce.

Realm Specific IP (RSIP)

RSIP takes a different approach than NAT to provide connectivity between different realms [2, 3]. RSIP uses a special node that is aware of the different realms and can distinguish between the two.

In general terms, RSIP uses two entities, a RSIP server and a RSIP client. The RSIP server is present in both realms and can provide router functionality between the realms. It can also be the node assigning public addresses to private hosts. The RSIP client is a node within the private realm that can temporarily use a public address when communicating with public hosts. Hence, RSIP makes use of public addresses for both parties when communicating between the private and public realms, and does not perform any address translation.

An advantage of this scheme is that there is no need to deploy ALGs for applications since public realm addresses are used even for private clients. However, plain RSIP does not allow public realm initiated connections.

There are two flavors of RSIP, namely Realm Specific Address IP (RSA-IP) and Realm Specific Address and Port IP (RSAP-IP).

Realm Specific Address IP (RSA-IP)

An RSA-IP client is assigned a public IP address when communicating with the public realm. This procedure is a one-to-one mapping and hence, no other host can use the address until it is released by the client (so-called address granularity). The packets are typically tunneled through the private realm to the RSA-IP server or they can be tunneled end-to-end.

Realm Specific Address and Port IP (RSAP-IP)

RSAP-IP operates similar to RSA-IP with the difference that RSAP-IP clients are assigned public IP addresses as well as associated ports (so-called port granularity). This way, several RSAP-IP clients can share public IP addresses. The multiplexing is performed through adding both an IP tunnel and an additional transport header with the assigned port as identifier if the public host terminates the tunnel. If the RSAP-IP server terminates the tunnel, the multiplexing is based on both destination address and port.

NAT-PT

Another flavor of NAT, called NAT-PT, adds specific protocol translation between IPv4 and IPv6. NAT-PT comes in three flavors corresponding to standard NAT, NAPT and bi-directional NAT. Bi-directional NAT-PT has support for public realm initiated communication, but with a one-to-one mapping of public IP address to private realm host. However, this scheme also does not scale very well due to the limited number of available public IPv4 addresses.

In general, public-realm initiated communication is enabled by manually and statically configuring the gateway such that an inside-bound packet with a given destination address and port will be forwarded to a certain node in the private realm. This scheme is generally referred to as static port mapping.

Bridging between a private realm and a public realm could also be effectuated on the session level, e.g. as described in [4].

Apparently, there are limitations regarding the number of simultaneous flows that can be supported by the gateway, as well as limitations regarding the mechanisms for establishing a connection initiated from nodes in the public realm.

SUMMARY OF THE INVENTION

None of the existing schemes meets the demands for supporting a massive deployment of a vast number of IP-enabled terminals in future networks, or more generally the demands for efficiently providing connectivity between networks of different address realms.

The present invention overcomes these and other drawbacks of the prior art arrangements.

It is a general object of the invention to provide an improved scheme for providing connectivity between networks of different address realms.

It is particularly important to provide enhanced scalability, for example to enable support of a large number of private nodes by means of a limited number of available public addresses. In other words, it is highly desirable to improve the multiplexation characteristics of a communication gateway.

It is also an object of the invention to provide stable support for flexible so-called outside-realm initiated communication, for example public-realm initiated connections.

Another object of the invention is to provide an improved method and system for establishing a connection between an outside address realm and an inside address realm through an intermediate gateway.

A particular object of the invention is to provide an improved gateway system for efficiently providing connectivity between different address realms.

Yet another object of the invention is to provide a gateway resource manager for supporting enhanced scalability and/or efficient and flexible outside-realm initiated communication.

These and other objects are met by the invention as defined by the accompanying patent claims.

The invention generally concerns the issue of providing connectivity between two different address realms, generally referred to as an inside realm and an outside realm, by establishing connections through an intermediate gateway. The gateway normally has a number of outside-realm gateway addresses for enabling representation of inside-realm nodes in the outside realm. Typically, the inside realm is a private address realm, whereas the outside realm is a public address realm. However, both the inside realm and the outside realm may be different private address realms, or alternatively both realms may be different public domains.

In this respect, it is a challenge to enable outside-realm initiated connections in a flexible and efficient manner. It is also a challenge to be able to support as many connections as possible through the gateway using a limited number of outside-realm addresses, both for inside-realm initiated as well as outside-realm initiated communication.

A basic idea according to a first aspect of the invention is to enable support for flexible outside-realm initiated communication by dynamically establishing new gateway connection states triggered, for each new connection, by a respective user-resource identifier query initiated from a corresponding outside node.

Preferably, an outside node that wants to initiate a new connection to an inside node prepares a user-resource identifier query, such as a DNS (Domain Name Server) query or equivalent, for transfer to a central allocation or addressing mechanism, which determines inside-realm network address information based on the inside node identifier included in the query. The identifier query from the outside node further includes predetermined connection information such as outside node address information and/or inside node port information. This predetermined connection information from the identifier query may then be used as a basis for identifying an outside-realm gateway address suitable for establishing a new dynamic gateway connection state for a flow between the outside node and the inside node through the gateway. The new dynamic gateway connection state is subsequently established at least partly based on the identified outside-realm gateway address, the predetermined connection information from the identifier query and the inside-realm network address information. In this way, the invention provides support for dynamic outside-realm initiated communication.

Examples of a user-resource identifier query include a DNS query, a URI (Universal Resource Identifier) query of the SIP (Session Initiation Protocol) protocol or similar query of a proprietary protocol such as a proprietary peer-to-peer protocol for multimedia communications, file sharing or computer games.

For an outside-realm initiated connection, the dynamic gateway connection state is typically, although not necessarily, established in two steps. First, a partially complete gateway connection state is created based on the identified outside-realm gateway address, the predetermined connection information from the identifier query and the inside-realm network address. Upon receipt of a packet from the outside node, the partially complete gateway state is transformed into a complete gateway connection state based on complementary connection information associated with the packet. The outside node is generally notified of the identified outside-realm gateway address to enable communication of the initial packet in the communication flow to the gateway.

The predetermined connection information used for identifying a suitable outside-realm gateway address may be an outside network address related to the initiating outside node. In this case, the complementary connection information for completing the gateway connection state preferably includes a port number related to the inside node as well as a port number related to the outside node.

As an alternative or as a complement, it has been recognized that it is possible to include information of the port at which the inside node listens for incoming packets, a predefined port or a port made known to the outside node by signaling, in the identifier query from the outside node. This inside node port information can then be used in the identification of an outside-realm gateway address. In this case, the complementary connection information for completing the gateway connection state typically includes an outside network address related to the outside node and an associated port number, or at least the outside node port number.

Advantageously, the task of setting up a new outside-realm initiated connection is functionally divided between the outside node, which sends the initiating identifier query, an identifier-to-address translator, a gateway resource manager and the actual gateway. The gateway resource manager is typically responsive to information such as the determined inside-realm network address corresponding to the relevant inside node and the predetermined connection information originally included in the identifier query, and responsible for identifying a suitable outside-realm gateway address to be used for establishing a new dynamic gateway connection state based on this information. The gateway resource manager finally sends a state set-up request to the gateway, which establishes the dynamic gateway connection state.

A basic idea according to a second aspect of the invention consists in intelligently using additional multiplexation information in the process of setting up new dynamic gateway connection states such that the number of connections that can be simultaneously supported by the gateway can be significantly increased. The additional multiplexation information is generally predetermined connection information that includes network address information and/or port information, and the main objective is to identify further connection information including an outside-realm gateway address based on the given address and/or port information. More particularly, the idea is to identify further connection information that in combination with the predetermined connection information defines an outside-realm gateway state representation that has no counterpart in a predetermined set of existing gateway connection states. By outside-realm gateway state representation is meant the outside-realm part of the overall gateway state representation.

For outside-realm initiated connections, the process of identifying further connection information is preferably performed with the aim to identify an outside-realm gateway address, which in combination with the predetermined connection information defines a partially complete outside-realm gateway state representation that has no counterpart in any existing partially complete gateway connection state. For example, the predetermined connection information is extracted from the identifier query as indicated above. Once such a gateway address has been identified, the gateway connection state is ready to be established based on the partially complete outside-realm representation defined by the outside-realm gateway address and the predetermined connection information. The additional multiplexation information, such as outside node address information and/or inside node port information, makes it possible to distinguish a much larger number of simultaneous connections compared to any of the prior art arrangements. The above process of increasing the multiplexation characteristics of the gateway normally requires a comparison in relation to all partially complete gateway connection states currently existing in the gateway. This comparison could be performed by the gateway resource manager directly in relation to the gateway, requesting and extracting the partially complete gateway states from the gateway as and when required. However, in order to reduce the signaling between the gateway and the resource manager, a separate list representation of existing partially complete gateway connection states is preferably maintained in the resource manager, or at least accessible by the resource manager.

A similar approach for obtaining support for a much larger number of simultaneous connections through the gateway can be applied also for inside-realm initiated connections.

The idea here is to identify, based on predetermined connection information including outside node address information and/or outside node port information, further connection information including an outside-realm gateway address, which in combination with the predetermined connection information defines an at least partially complete outside-realm gateway state representation that has no counterpart in any existing gateway connection state. Establishment of the connection can then be initiated based on the generated outside-realm representation.

For inside-realm initiated connections, the process of increasing the multiplexation characteristics of the gateway typically requires a comparison in relation to all existing gateway connection states, not only in relation to partially complete gateway states as for outside-realm initiated connections.

For so-called substitution style gateways based on address and port translation, the further connection information to be identified may also include associated gateway port information in addition to the outside-realm gateway address. In this case, the resulting outside-realm representation is a complete outside-realm representation, which together with a corresponding inside-realm representation completely defines the new connection through the gateway.

On the other hand, for so-called relaying style gateways, where the inside-realm representation of the gateway state may be a virtual point-to-point interface, the resulting outside-realm representation is only a partially complete representation, which forms the basis for creating a partially complete gateway state. In this case, upon receipt of a packet from the inside node, it is normally recommended to check that the partially complete representation in further combination with inside node port information associated with the received packet defines a unique complete outside-realm representation that can be used for completing the gateway connection state.

The multiplexation gain offered by the invention is truly significant, leading to a support for a considerably larger number of simultaneous connections compared to any of the prior art schemes. In fact, the invention and the advantages it offers may even render a fast introduction of the IPv6 protocol completely unnecessary.

The invention, in all its aspects, is applicable to any suitable communication gateway known to the art, ranging from NAT-based gateways, or more generally substitution style gateways to RSIP-based gateways, or more generally relaying style gateways.

The invention offers the following advantages:

- Dynamic, flexible and efficient outside-realm initiated communication.
- Efficient use of user-identifier queries, such as DNS-queries, in the overall process of establishing outside-realm initiated connections.
- Improved gateway multiplexation characteristics.
- Support for a much larger number of simultaneous connections through the gateway compared to prior art gateways, both for outside-realm and inside-realm initiated connections.
- Enhanced scalability, for example to enable support of a large number of private nodes by means of a limited number of available public addresses.
- Generally applicable to most types of gateways.

Other advantages offered by the present invention will be appreciated upon reading of the below description of the embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further objects and advantages thereof, will be best understood by reference to the following description taken together with the accompanying drawings, in which:

FIG. **1** is a schematic diagram illustrating a gateway interconnecting a private network and a public network;

FIG. **2** illustrates a basic model of an exemplary gateway providing connectivity between an inside-realm network and an outside-realm network;

FIG. **3** is a schematic flow diagram of a method for enabling support for flexible outside-realm initiated communication according to a preferred embodiment of the invention;

FIG. **4** is a schematic flow diagram of a basic method for improving the gateway multiplexation characteristics for outside-realm initiated communication according to a preferred embodiment of the invention;

FIG. **5** is a schematic flow diagram of a basic method for improving the gateway multiplexation characteristics for inside-realm initiated communication according to a preferred embodiment of the invention;

FIG. **6** is a schematic diagram of an exemplary gateway system, including a gateway and an associated gateway resource manager, providing effective support for improved gateway multiplexation characteristics;

FIG. **7** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of inside-realm initiated communication through a substitution style gateway;

FIG. **8** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of inside-realm initiated communication through a relaying style gateway;

FIG. **9** is a schematic diagram illustrating an example of an overall system for enabling support for flexible and efficient outside-realm initiated connections according to a preferred embodiment of the invention;

FIG. **10** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication through a substitution style gateway, using outside node address information for efficient multiplexation;

FIG. **11** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication through a substitution style gateway, using inside node port information for efficient multiplexation;

FIG. **12** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication through a relaying style gateway, using outside node address information for efficient multiplexation;

FIG. **13** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication through a relaying style gateway, using inside node port information for efficient multiplexation;

FIG. **14** is a schematic block diagram illustrating an implementation example of a system for providing connectivity between nodes of different address realms according to a particular embodiment of the invention; and

FIG. **15** is a schematic block diagram illustrating an implementation example of a system for providing connectivity

between nodes of different address realms according to another particular embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Throughout the drawings, the same reference characters will be used for corresponding or similar elements.

General Overview

In general, there is a demand for providing connectivity between different address realms, more generally referred to as an outside realm and an inside realm. To this end, there is normally provided an intermediate gateway, which has a number of outside-realm gateway addresses for enabling outside-realm representation of inside-realm nodes. In many practical applications, the inside realm is a private address realm [5], whereas the outside realm is a public address realm. In other applications, however, the inside realm and the outside realm may be different private address realms, or alternatively different public domains.

In this respect, a public realm network is generally a network having communication nodes together with an associated network address space consisting of globally unique network addresses. A private realm network on the other hand is a network having nodes together with an associated network address space consisting of possibly non-unique network addresses, in the sense that two nodes in different instances of a private realm may be assigned the same network address.

A gateway is generally a network element that is connected to both an inside realm and an outside realm. As previously mentioned, there are different types of gateways, especially substitution style gateways (including different flavors of NAT) and relaying style gateways (including different flavors of RSIP). It should also be understood that the overall gateway function includes not only layer 4 packet forwarding, but could encompass packet forwarding on any network layer including also layer 3 packet forwarding.

For a better understanding of the invention, it may be useful to begin with a brief introduction of a basic model of an exemplary gateway providing connectivity between an inside realm and an outside realm, referring to FIG. **2**.

FIG. **2** illustrates a basic model of an exemplary gateway **30** interconnecting an inside realm **10** and an outside realm **20**. The gateway **30** is associated with a gateway resource manager **40**, which among other things manages the pool of outside-realm network addresses that have been allocated to the gateway. In the gateway **30**, the basic gateway functions are supported by an outside-bound process element **32**, an inside-bound process element **34** and a packet forwarding element **36**. The gateway **30** and gateway resource manager **40** may be implemented in separate, but interconnected nodes. Alternatively, the gateway resource manager **40** may be co-located with the gateway **30**, even integrated in the gateway.

For a substitution style gateway, as the name indicates, substitution of address and port information in the packet headers is performed to enable proper packet forwarding. A gateway connection state in a substitution style gateway is normally represented by an outside n-tuple and an inside n-tuple. In general, an n-tuple is a set of n information elements that typically include: (a source network address, a source port number, a destination network address, a destination port number, a protocol number). An outside n-tuple is typically an n-tuple with the source and destination network addresses belonging to the outside realm. An inside n-tuple is typically an n-tuple with the source network address belonging to the inside realm and the destination network address belonging to the outside realm. To enable proper packet forwarding for communication flows, there are two basic classification processes:

- The inside-bound process, in which each inside-bound packet is matched against the outside n-tuples of the gateway connection states in the gateway, and when finding a matching outside n-tuple, the destination address and port of the packet header are substituted with the source address and port of the inside n-tuple corresponding to the identified outside n-tuple.
- The outside-bound process, in which each outside-bound packet is matched against the inside n-tuples of the gateway connection states in the gateway, and when finding a matching inside n-tuple, the source address and port of the packet header are substituted with the destination address and port of the outside n-tuple corresponding to the identified inside n-tuple.

For a relaying style gateway, a gateway connection state is normally represented by an outside n-tuple and a virtual point-to-point interface towards a communication node on the inside realm. An example of a virtual point-to-point interface is an IP-in-IP tunnel in which, in the inside-bound direction, a packet is encapsulated in another packet, with destination address equal to the inside node address, and source address equal to the inside gateway address, and in the outside-bound direction the incoming packet is decapsulated, whereby an inner packet is extracted. In another example, instead of encapsulation and decapsulation, there could be a layer 2 point-to-point link between the gateway and the communication node on the inside realm (for example, in a GPRS system, the PDP Context layer).

In a relaying style gateway, the two basic processes for enabling proper packet forwarding for communication flows are defined as:

- The inside-bound process, in which each inside-bound packet is matched against the outside n-tuples of the gateway connection states in the gateway, and when finding a matching outside n-tuple, the packet is sent to the virtual point-to-point interface corresponding to the identified outside n-tuple.
- The outside-bound process, in which each outside-bound packet comes in on a virtual point-to-point interface and forwarded by the gateway to the outside realm.

The main difference between substitution and relaying style is that in relaying style, the inside node is aware of the currently allocated outside-realm address (and port number(s)). In substitution style, the inside-realm node is not aware of the outside-realm address, and instead the gateway performs transparent translation (substitution).

In both substitution and relaying style gateways, there may be partially complete gateway connection states, i.e. states which represent connections that currently are in the process of being established, but which have not yet collapsed into a complete gateway connection state for a gateway session. Such partially complete gateway states are sometimes referred to as gateway gates or pinholes.

In a substitution style gateway, a gateway gate is a gateway connection state with an outside n-tuple and an inside n-tuple, where the outside n-tuple and/or the inside n-tuple has one or more unspecified connection variables (wild cards, denoted by "*"). When the gateway receives an inside-bound packet/outside-bound packet matching the specified values of the partially complete outside/inside n-tuple, that n-tuple is completed in the sense that the up-to-now unspecified values of

the partially complete n-tuple are fixed to the corresponding values associated with the packet.

In a relaying style gateway, a gateway gate is a gateway connection state with an outside n-tuple and an inside n-tuple, where the outside n-tuple and/or the inside n-tuple has one or more unspecified connection variables. When the gateway receives an inside-bound packet matching the specified values of the partially complete outside n-tuple, that n-tuple is completed in the sense that the up-to-now unspecified values of the partially complete n-tuple are fixed to the corresponding values associated with the packet.

An outside n-tuple is generally also referred to as an outside-realm gateway state representation, since it refers to the part of the overall gateway state representation that is related to the outside realm.

With the above basic insights into the operation of a general gateway, the understanding of the sometimes rather complex aspects of the invention will now be somewhat facilitated and more straightforward.

As previously mentioned, it is a basic challenge to enable outside-realm initiated connections in a flexible and efficient manner. It is also highly desirable to improve the multiplexation characteristics of the gateway, both for inside-realm initiated as well as outside-realm initiated communication. The main objective in the latter respect is to be able to support as many connections as possible through the gateway using a limited number of outside-realm addresses.

Exemplary Basic Procedures for Outside-Realm Initiated Communication

The inventors have recognized that a flexible and dynamic mechanism for enabling outside-realm initiated communication is obtained by letting a user-resource identifier query, such as a DNS-query or equivalent query, initiated from an outside node trigger the set-up of a connection state in the gateway. A basic procedure according to a preferred embodiment of the invention is generally outlined in the flow diagram of FIG. **3**. In step **S1**, an outside node that wants to initiate a new connection to a particular inside node prepares a user-resource identifier query, such as a DNS query or equivalent, for transfer to a central allocation or addressing mechanism. In step **S2**, an inside-realm network address is determined for the inside node based on an inside node identifier included in the query. In the case of a DNS-query, this may for example be accomplished by a conventional domain-name-to-network-address translator. The identifier query further includes predetermined connection information that is handled by a gateway resource manager, which uses this information as a basis for identifying an outside-realm gateway address suitable for establishing a new dynamic gateway connection state, as indicated in step **S3**. The predetermined connection information may for example be the network address of the outside node or inside node port information. In the latter case, the port information may be a pre-defined inside node receiver port, or a receiver port number made known to the outside node by explicit signaling. Next, in step **S4**, the new dynamic gateway connection state for a flow between the outside node and the inside node through the gateway is established at least partly based on the identified outside-realm gateway address, the predetermined connection information and the inside-realm network address. This means that the invention provides support for dynamic outside-realm initiated communication. Among other things, this allows all forms of push services, notification services and instant messaging services.

For an outside-realm initiated connection, the dynamic gateway connection state is typically, although not necessarily, established in two steps. First, a partially complete gateway connection state is created based on the identified outside-realm gateway address, the predetermined connection information extracted from the identifier query as well as the inside network address. Upon receipt of a packet from the outside node, the partially complete gateway state "collapses" into a complete gateway connection state as complementary connection information such as address and/or port information in the packet header is used to fill-in the unspecified parts of the gateway state. The outside node is generally notified of the identified outside-realm gateway address to enable communication of the initial packet towards the gateway.

Improved Gateway Multiplexation Capacity

In a further aspect of the invention, the number of ontside-realm initiated connections that can be simultaneously supported by the gateway can be significantly increased by intelligently using one or more additional multiplexation variables in the process of setting up new dynamic gateway connection states. Here, the additional multiplexation information preferably includes the predetermined connection information, typically outside node address information and/or inside node port information, as extracted from the initiating user-resource identifier query. However, from the viewpoint of the gateway resource manager, the origin of the predetermined connection information to be used in the state set-up process is not critical, as long as it receives proper connection information.

FIG. **4** is a schematic flow diagram of a basic method for improving the gateway multiplexation characteristics for outside-realm initiated communication according to a preferred embodiment of the invention. In the following, an outside-realm gateway address is simply referred to as an outside gateway address.

As indicated in step **S11**, the exemplary method involves receiving predetermined connection information to be used in the state set-up process. For a substitution style gateway, further connection information, typically an outside gateway address, is selected in step **S12**. In order to avoid a gateway resource clash between several simultaneous on-going connection set-ups, the partially complete outside n-tuple, defined by a combination of the outside gateway address and the predetermined connection information, is analyzed in comparison to all existing partially complete gateway connection states, as indicated in step **S13**. The analysis includes checking whether the above combination of connection information, defining a partially complete outside n-tuple, has any counterpart in the existing partially complete gateway connection states. If the partially complete outside n-tuple is already present (Y) in an existing partially complete gateway state, there is already a binding between the outside gateway address and the predetermined connection information. This generally means that another outside gateway address has to be selected from the gateway address pool, repeating steps **S12**-**S13**. The gateway resource manager repeats the process with the next address in the outside gateway address pool until a "free" address is found or the end of the address pool is reached. If it is possible to identify an outside gateway address, which in combination with the predetermined connection information has no counterpart in any existing partial gateway state (N), the procedure continues with step **S14**. In step **S14**, connection establishment is initiated based on the partially complete outside n-tuple (and naturally also the corresponding inside representation), awaiting completion in step **S15** upon receipt of the first packet in the communication flow.

If all outside gateway addresses in the address pool has been traversed without finding a unique partial outside n-tuple, the connection request may have to be rejected. It is however also possible to start traversing the addresses in gateway address pool once again, assuming that the delay of the mentioned selection procedure should minimize the risk of two connections being set-up simultaneously so that any existing data connection establishment should have had time to be completed upon receipt of the first packet.

As mentioned above, when the first packet arrives, the partial gateway state turns into a complete gateway connection state. Complete gateway connection states can be further distinguished by complementary connection information associated with the corresponding packets, and so do not have to be represented in the list used in step **S13**. Therefore, as soon as there is a complete binding, when a partial gateway state turns into a complete gateway state, that partial gateway state is removed from the list of ambiguity candidates.

The above process of increasing the multiplexation characteristics of the gateway apparently requires a comparison in relation to all partially complete gateway connection states currently existing in the gateway. This comparison could be performed by the gateway resource manager directly in relation to the gateway, requesting and extracting the partially complete gateway states from the gateway as and when required. However, in order to reduce the signaling between the gateway and the resource manager, a separate list representation of existing partially complete gateway connection states is preferably maintained in the resource manager, or at least accessible by the resource manager.

For relaying style gateways, it should be understood that the inside-realm nodes are generally aware of the outside-realm addresses they are using, meaning that such outside-realm addresses have typically been pre-allocated to the inside nodes. This means that for relaying style gateways, step **S12** is performed earlier in the overall chain of events, and that step **S13** becomes more of a check whether the combination of a pre-allocated outside gateway address and received predetermined connection information has any counterpart among the existing partially complete gateway states.

Exemplary Scenarios

For example, consider public host B that wants to connect to two private nodes **A1** and **A2**. Host B initiates a connection set-up towards node **A1**, and the gateway resource manager finds a free outside gateway address, say **aOG1**. Simultaneously, host B initiates a connection set-up towards node **A2**, and the gateway resource manager attempts to identify a useful outside gateway address. By using inside node receiver port information in the gateway address identification process, it is possible, assuming that private nodes **A1** and **A2** do listen on different port numbers, to assign the same public gateway address, **aOG1**, for pending connections towards both private nodes **A1** and **A2**, since now the two pending connections can be distinguished based on the destination port information **pA1** and **pA2**. Consequently, this means that each public gateway address can be used for any number of private nodes, as long as they all listen on different port numbers.

Assume furthermore that public host B wants to initiate connections to yet another private node **A3**, listening on the same port number as node **A1**. Provided that the connection between host B and node **A1** has already been completely established when host B initiates a connection set-up towards node **A3**, it is actually safe to select the same public gateway address for node **A3**, since it can be safely assumed that host B will use different port numbers when sending traffic towards the private nodes **A1** and **A3**. The port number of public host B is appended as source port information in the packet header, and can be used as complementary connection information for distinguishing a given packet flow from other flows from B.

In another example, consider two public hosts **B1** and **B2**, each wanting to connect the same private network hidden behind a gateway. Host **B1** initiates a connection set-up, and the gateway resource manager finds a free public gateway address, say **aOG1**. Simultaneously, host **B2** initiates a connection set-up, and the gateway resource manager attempts to identify a useful public gateway address. By using the public host address in the process of identifying a useful outside gateway address, the same gateway address can be selected for host **B2**, since the two pending connections can be distinguished based on the source address information, **aOB1** and **aOB2**. In general, this in fact means that each public gateway address can be used for any number of different public hosts.

Assume furthermore that public host **B1** wants to initiate connections to two different private nodes **A1** and **A2**. Provided that the connection between host **B1** and node **A1** has already been completely established when host **B1** initiates a connection set-up towards node **A2**, it is actually safe to select the same public gateway address for node **A2**, since it can be safely assumed that host **B1** will use different port numbers when sending traffic towards the private nodes **A1** and **A2**. The port number of public host **B1** is appended as source port information in the packet header, and can be used as complementary connection information for distinguishing a given packet flow from other flows from **B1**. This even allows private nodes **A1** and **A2** to listen on the same port number. It is a clear advantage to be able to allow the application software in the private nodes to choose port freely.

Lower Complexity Implementation

If a lower degree of implementational complexity is desired, with a lower impact on existing gateway implementations, it is possible to eliminate the step-wise state set-up and establish a complete gateway connection state directly based only on the available connection information before packet reception. In a preferred lower-complexity implementation, the gateway resource manager requests allocation of a public gateway address to a given private node, but only for traffic coming from a particular public host, still keeping the public gateway address available for traffic to the same or other private nodes from other public hosts. Naturally, the drawback is that for flows coming from one particular public host, the number of private nodes that can simultaneously receive information is limited to the number of available public gateway addresses. However, flows originating from different public hosts can still be allocated the same public gateway address.

Exemplary Basic Procedures for Inside-Realm Initiated Communication

Improved Gateway Multiplexation Capacity

A similar approach for supporting a much larger number of simultaneous connections through the gateway can be applied also for inside-realm initiated connections, as generally outlined in the basic flow diagram of FIG. **5**. In step **S21**, predetermined connection information including outside node address information and/or outside node port information, is received by the gateway resource manager. For a substitution style gateway, further connection information including at least an outside gateway address is selected in step **S22**. In step **S23**, it is tested whether the combination of

the predetermined connection information and the further connection information, together defining an at least partially complete outside-realm representation of a new gateway connection state to be established, has any counterpart in the existing gateway connection states. If the at least partially complete outside n-tuple is already present (Y) in an existing gateway state, another outside gateway address has to be selected from the gateway address pool, repeating steps **S22**-**S23**. The gateway resource manager repeats the process with the next address in the outside gateway address pool until a "free" address is found or the end of the address pool is reached. If it is possible to identify an outside gateway address, which in combination with the predetermined connection information defines an at least partially complete outside n-tuple that has no counterpart in any existing gateway state (N), the procedure continues with step **S24**. In step **S24**, connection establishment is initiated based on the at least partially complete outside n-tuple (and naturally also the corresponding inside representation).

It should be especially noted that, for inside-realm initiated connections, a comparison in relation to all existing gateway connection states is typically required, not only in relation to partially complete gateway states as for outside-realm initiated connections.

For so-called substitution style gateways based on address and port translation, the further connection information to be identified may also include associated gateway port information in addition to the outside gateway address. In this case, the resulting outside-realm representation is a complete outside-realm representation, which together with a corresponding inside-realm representation completely defines the new connection through the gateway.

On the other hand, for so-called relaying style gateways, where the inside-realm representation of the gateway state may be a virtual point-to-point interface, the resulting outside-realm representation is normally only a partially complete representation. This partially complete outside-realm representation forms the basis for creating a partially complete gateway state, which is subsequently transformed into a complete gateway state upon receipt of the first packet from the inside node. In addition, as previously mentioned, for relaying style, the inside-realm nodes are generally aware of the outside-realm addresses they are using, which means that outside-realm addresses have already been pre-allocated.

The Gateway Resource Manager

The above processes of increasing the multiplexation characteristics of the gateway in order to be able to distinguish a much larger number of simultaneous connections compared to any of the prior art systems, apparently requires a comparison in relation to various sets of gateway connection states currently existing in the gateway. Referring to the simplified block diagram of FIG. **6**, this comparison could be performed by the gateway resource manager **40** directly in relation to the gateway **30**, requesting and extracting the relevant gateway states from a state database **38** in the gateway as and when required. However, in order to reduce the signaling between the gateway **30** and the resource manager **40**, the analysis is preferably performed in relation to one or more separate list representations of the relevant gateway connection states. This list representation **42** is conveniently maintained in the resource manager **40**, or at an external location that makes it possible for resource allocation logic **44** in the resource manager to effectively access the information.

In general, the resource manager may be implemented as software, hardware, firmware or any combination thereof. In the case of a software-implementation, the steps, functions and actions related to the resource manager are mapped into a computer program, which when being executed by a computer or equivalent processing system effectuates the relevant resource allocation.

Sequence Diagrams for Inside-realm Initiated Communication

For a more detailed understanding of the invention, the invention will now be described with reference to exemplary signal sequence diagrams. For simplicity, we will start with inside-realm initiated communication.

Substitution Style

FIG. **7** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of inside-realm initiated communication through a substitution style gateway. The gateway (GW) can enable communication initiated from a node A on the inside realm towards a node B on the outside realm. It is assumed that node A has obtained information of the destination network address aOB, typically through a conventional DNS-query based on a FQDN. The destination port number pB may be a well-known port number, or made known by explicit signaling. An exemplary sequence for supporting a communication flow between A and B through the gateway could be:

1. Node A has the network address aIA and chooses the source port (ephemeral port) pA. The gateway (GW) receives the first packet in a certain communication flow initiated from the inside realm.
2. The gateway sends a request including the destination network address aOB and/or port number pB to the gateway resource manager (GRM).
   In process X, the gateway resource manager allocates a network address aOG from the gateway address pool and given that address preferably also a port number pG from the gateway port pool based on the destination address aOB and/or destination port pB.
   The gateway typically supplies the destination address and/or destination port as predetermined connection information to the gateway resource manager, which investigates whether there is a binding between the next gateway address in the gateway address pool and the destination address and/or destination port. If such a binding exists, the resource manager repeats the process with the next gateway address in the pool until a free gateway address without binding is found (or the end of the gateway address pool is reached).
   In this particular example, the GRM manager executes an algorithm that attempts to select aOG and pG so that the outside n-tuple (src:(aOB, pB); dest:(aOG, pG); . . .) is not an outside n-tuple of an already existing gateway connection state.
3. The allocated gateway address aOG and the associated port number pG are sent back to the gateway.
   In process a, the gateway creates a new gateway connection state based on the available connection information. The inside n-tuple gets the values: (aIA, pA; aOB, pB) and the outside n-tuple gets the values: (aOB, pB; aOG, pG).
4. The packet is processed in the gateway by the outside-bound process, and forwarded through the gateway to the outside-realm node B.
5. A reply packet in the communication flow is received by the gateway from node B.
6. The reply packet is processed by the inside-bound process, and delivered to the inside-realm node A.

The multiplexation capacity is improved beyond the limitations of the prior art, and the number of flow can be greater

than (number of network address in the gateway address pool)·(number of usable ports).

Relaying Style

FIG. **8** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of inside-realm initiated communication through a relaying style gateway.

For relaying style it is desirable, although not necessary, to avoid the port granularity alternative by ensuring sufficient port multiplexing for the address granularity alternative. Especially in the case of communication initiated in the outside realm, as described later on with reference to FIGS. **12** and **13**, the receiving inside node should preferably be able to choose port number freely. This is not satisfied in the port granularity alternative. Therefore, in the following we mainly refer to the address granularity alternative when discussing the relaying style option.

An exemplary sequence for supporting a communication flow from inside nodes A**1** and A**2** to outside node B through the gateway could be:

1. Node A**1** wants to initiate a communication flow towards node B, which belongs to the outside realm. Node A**1** sends a request including the destination network address aOB and port number pB to the gateway (GW). In the IETF RSIP framework (RFC3103), this message could be the "ASSIGN_REQUEST_RSA-IP".
2. The gateway sends a request to the gateway resource manager (GRM).
   In process X, the GRM manager allocates a network address aOG from the gateway address pool.
   The gateway typically supplies the destination address and/or destination port as predetermined connection information to the gateway resource manager. In this example, both destination address information and port information are included in the request. To improve the multiplexing capacity, the gateway resource manager executes an algorithm that given aOB and pB attempts to select aOG so that outside n-tuple (src:(aOB, pB); dest: (aOG, *); . . .) is not an outside n-tuple of an already existing gateway connection state. If that is not possible (all possible gateway addresses aOG are already used), select the gateway address that is utilized in the least number of gateway connection states.
3. The allocated gateway address aOG is sent back to the gateway.
4. In process a, the gateway creates a new partially complete gateway connection state based on the available connection information. The inside-realm representation is denoted by A**1** and represents a virtual point-to-point link to the inside node A**1**, whereas the outside n-tuple gets the values: (aOB, pB; aOG, *). The "*" means that this field is for the time being unspecified.
   A reply is sent back to node A**1**, including the allocated gateway address aOG.
5. Node A**2** also wants to initiate a communication flow towards node B, and sends a request including the destination network address aOB and port number pB to the gateway (GW).
6. The gateway sends a corresponding request to the gateway resource manager (GRM).
   In process Y, the GRM manager allocates a network address aOG from the gateway address pool, preferably by using the same algorithm as in process X described above. Assume, for illustrative reasons, that all gateway addresses in the gateway address pool have been traversed without finding a completely "free" address, forcing the resource manager to select the least utilized gateway address. In this example, further assume that the least utilized address is the same address aOG that was previously allocated to node A**1**.
7. The allocated gateway address aOG is sent back to the gateway.
8. In process b, the gateway creates a further partially complete gateway connection state. The inside-realm representation is denoted by A**2** and represents a virtual point-to-point link to the inside node A**2**, whereas the outside n-tuple gets the values: (aOB, pB; aOG, *). The "*" means that this field is for the time being unspecified.
   A reply is sent back to node A**2**, including the allocated gateway address aOG.
9. Node A**1** selects a source port pA**1** (a so-called ephemeral port) for the communication flow, and sends the first packet. This packet is received by the gateway.
   In process c, the corresponding partially complete outside n-tuple collapses into a complete outside n-tuple (aOB, pB; aOG, pA**1**), whereby the up-to-now unspecified value in the outside n-tuple is filled-in with the value pA**1**.
10. The packet is processed by the outside-bound process, and forwarded through the gateway to the outside-realm node B.
11. A reply packet in the communication flow is received by the gateway from node B.
12. The packet is processed by the inside-bound process of the gateway and delivered to node A**1**.
13. Node A**2** selects a source port pA**2** (a so-called ephemeral port) for the communication flow, and sends the first packet. This packet is received by the gateway.
    In process Z, it is investigated whether pA**2** is equal to pA**1**. If pA**2**=pA**1**, there is a collision and the second partially complete gateway connection state (in box c) should not be collapsed. Instead, the gateway should preferably try to influence node A**2** to select another pA**2** by resetting the communication flow, e.g. by sending a TCP reset signal.
    Assuming that pA**2** differs from pA**1**, the partially complete outside n-tuple collapses in process d into a complete outside n-tuple (aOB, pB; aOG, pA**2**), whereby the up-to-now unspecified value in the outside n-tuple is filled-in with the value pA**2**.
14. The packet is processed by the outside-bound process, and forwarded through the gateway to the outside-realm node B.
15. A reply packet in the communication flow is received by the gateway from node B.
16. The packet is processed by the inside-bound process of the gateway and delivered to node A**2**.

The multiplexing capacity can be increased to a point where the address granularity alternative can be used instead of the port granularity alternative. This means that arbitrary ephemeral port numbers can be used.

In the following, the invention will be described with reference to outside-realm initiated communication triggered by a DNS-query or equivalent user-resource identifier query.

Exemplary Basic Block Diagram for Outside-Realm Initiated Communication

For a better understanding of the complex mechanisms involved in the invention, it is useful to begin with an exemplary overall system overview, referring to FIG. **9**.

FIG. **9** is a schematic diagram illustrating an example of an overall system for enabling support for flexible and efficient outside-realm initiated connections according to a preferred

embodiment of the invention. The exemplary overall system for interconnecting an inside node A and an outside node B comprises an intermediate gateway **30**, an associated gateway resource manager **40**, a name-to-address (N/A) translator **50** or equivalent translator together with an associated AAA-server **60**. The N/A-translator **50** may for example be a modified DNS server, which accepts a query including a name, and finally responds with a reply including a network address belonging to the outside realm. Optionally, the query and reply also include port number information. A name is a globally unique string that is associated to each node. For example, the name of a communication node could be a FQDN (Fully Qualified Domain Name) formed as a mobile telephone number, MSISDN, together with the operator's domain name, e.g. "070123456789.operator.country". The AAA-server **60** includes functionality for managing dynamic profile data, including name information and inside-realm related network address information, for the communication nodes currently within the inside realm. More generally, the N/A-translator **50** is an identifier-to-address translator, accepting a general identifier query including a DNS-query, a SIP-URI-query [6] and similar query of any proprietary protocol.

In an exemplary basic scenario, a client application is started in an inside node A such as a mobile terminal or other node equipment. The client application opens a socket, i.e. a (low-level) networking interface, and starts listening on a port. Assume by way of example that the client has a private IPv4 address behind the gateway **30**, and that outside the gateway towards the outside node B, e.g. an application server of a service provider or other node equipment, normal public routing takes place. It is furthermore assumed that the mobile terminal or other equipment of node A has a name, or similar identifier, and that it has registered itself in the private inside realm so that the AAA-server **60** includes a profile with the name together with the private network address or equivalent symbol identifying a point-to-point interface. The application server of node B may know in advance what port number (a so-called well known or pre-defined port) the client software is listening to, or alternatively the client software may signal the port number to the public application server in a registration message. Node B normally also has knowledge of the name of node A.

In the example of FIG. **9**, control signaling interfaces are indicated by solid lines and packet data interfaces are indicated by dashed lines.

At first, the node B application server sends a DNS-query (1) or equivalent query to the N/A-translator **50**. The query also includes information on the public network address of node B and/or information about which port node A is listening to. The N/A-translator **50** sends a request (2) including the name of node A to the AAA-server **60**, which responds with a reply (3) including the private network address of node A, or equivalently a symbol representing a point-to-point interface to node A. The N/A-translator **50** then sends an allocation request (4) including the name and associated private network address representation of node A together with the public network address of node B and/or the inside node port number to the gateway resource manager (GRM) **40**. Based on this information, the gateway resource manager **40** identifies a suitable public gateway address for node A and sends a request (5) to the gateway (GW) **30** for creating a gateway connection state. After creating the gateway connection state, the gateway **30** sends a reply (6) confirming the state set-up to the resource manager **40**. The resource manager **40** then sends a reply (7) including the public gateway address allocated to node A towards the N/A-translator **50**, which in turn forwards this information in a final reply (8) to node B. The application server of node B now sends (9) the first packet to the gateway **30**, which if necessary picks up complementary connection information such as the port number used by node B and perhaps also the address of node B for enabling the gateway **30** to transform a possibly incomplete gateway connection state into a complete gateway state. Upon collapsing an incomplete gateway connection state, the gateway **30** preferably informs (10) the resource manager **40**, which in turn updates its list representation of gateway connection states. In the gateway **30**, the inside-bound process cooperates with the packet forwarding process to deliver the packet through the gateway **30** and onwards (11) to node A. Node A can reply (12) and send information through the gateway **30** and onwards (13) to node B.

It is also possible to provide the DNS-query directly to the gateway resource manager, which in turn forwards the name information to an associated name-to-address translator function that returns an inside network address related to the relevant inside node. As before, the gateway resource manager assigns a public gateway address to the inside node based on predetermined connection information included in the DNS-query and sends a DNS-reply including the assigned address to the requesting outside node.

From an implementational point of view the overall central addressing mechanism, including the name-to-address translator and the gateway resource manager, can be realized in a single process, in different processes running on a single node, or in different processes that are physically separated in several nodes.

If the outside node network address is used for identifying a suitable gateway address, it is recommended that the name query is delivered directly and not relayed by intermediate nodes. In the case when a DNS server is used for name look-up, this corresponds to disabling so-called recursive look-ups by setting the RD (Recursive Desired) bit to "0", and instead rely on iterative look-ups. Uncontrolled caching should also be avoided by setting the TTL (Time-To-Live) parameter to a value smaller than the time distance between two consecutive flow initiations towards the same inside-realm node and port number.

As previously indicated, it may not be necessary to perform the state set-up in two phases. Instead, it is actually possible to establish a complete gateway connection state directly based on the available connection information including the outside node address and/or the inside node port, eliminating the need for the signaling indicated at (10). This obviously reduces the multiplexation gain somewhat since the outside node port number can not be used as a distinguishing parameter when setting up the gateway connection state. Such a solution may however be sufficient depending on the circumstances.

General mechanisms for controlling NAT/FW states have been proposed by the Internet Engineering Task Force working group on Middlebox Communication (MIDCOM).

Sequence Diagrams for Outside-Realm Initiated Communication

Substitution Style—Source Address Known

FIG. **10** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication through a substitution style gateway, using outside node (source) address information for efficient multiplexation.

In this example, the initial state is that a communication node A in the inside realm has started an application that is listening for incoming traffic on port number pA. Node A has the "name" nA. Node A has registered itself in the inside

realm so that the AAA-server has a profile that includes nA together with the network address (aIA) that is allocated to node A. A communication node B in the outside realm wishes to establish communication towards node A. Node B has knowledge of nA and pA.

In the following sequence, there are three inside nodes with names nA1, nA2, and nA3, inside-realm addresses aIA1, aIA2, and aIA3, listening to ports pA1, pA2, and pA3, respectively. Also, there are two outside nodes with outside-realm addresses aOB1 and aOB2, sending on ports pB1 and pB2, respectively.

1. Node B1 sends a query including nA1 to the N/A-translator. The address aOB1 is visible in the source field of the query packet.
2. The N/A sends a request including nA1 to the AAA-server.
3. The AAA-server looks up the network address, aIA1, corresponding to nA1 and sends a reply to the N/A including nA1 and aIA1.
4. The N/A sends a request including nA1, aIA1, and aOB1 to the gateway resource manager (GRM).

   In Process X, the gateway resource manager performs the following algorithm: In this case, it is assumed that there are no existing partial gateway states, also referred to as gates. The gateway resource manager can therefore freely select aOG from the gateway address list, usually taking the first available address.
5. The gateway resource manager sends a request to the gateway to create the partial gateway state (gate) described in box a.
6. The gateway replies after creating the partial gateway state.
7. The gateway resource manager sends a response including nA1 and aOG.
8. The N/A sends a response including nA1, aOG to node B1.
9. Node B2 sends a query including nA2 and aOB2 to the N/A. The address aOB2 is visible in the source field of the query packet.
10. The N/A sends a request including nA2 to the AAA-server.
11. The AAA-server looks up the network address, aIA2, corresponding to nA2 and sends a reply including nA2 and aIA2 to the N/A.
12. The N/A sends a request including nA2, aIA2, and aOB2 to the gateway resource manager.

    In Process Y, the gateway resource manager performs the following algorithm: Try to select aOG from the gateway address list so that the outside n-tuple (partly unspecified)(src:(aOB2,*); dest:(aOG,*); . . .) is not an outside n-tuple of an already existing partial gateway state. In this case, since aOB2 is not equal to aOB1, it's OK to select any aOG, even the same aOG as was selected in Process X above. If that would not have been the case, another aOG than that selected in Process X had had to be chosen.
13. The resource manager sends a request to the gateway to create the gateway state described on the second row in box b.
14. The gateway replies after creating the partial gateway state.
15. The resource manager sends a response including nA2 and aOG.
16. The N/A sends a response including nA2 and aOG to node B2.
17. Node B1 sends the first packet in the communication flow towards node A1.
18. In the gateway, the partial gateway state collapses into a complete gateway state, whereby the outside n-tuple is completed so that it is: (src:(aOB1, pB1); dest:(aOG, pA1); . . .) and the inside n-tuple is (src:(aIA1, pA1); dest:(aOB1, pB1); . . .), as seen in box c.
19. The packet is forwarded by the gateway towards node A1.
20. Node A1 sends the next packet in the communication flow towards node B1.
21. The packet is forwarded by the gateway towards node B1.
22. Node B1 sends a query including nA3 to the N/A. The address aOB1 is visible in the source field of the query packet.
23. The N/A sends a request including nA3 to the AAA-server.
24. The AAA-server looks up the network address, aIA3, corresponding to nA3 and sends a reply including nA3 and aIA3 to the N/A.
25. The N/A sends a request including nA3, aIA3, and aOB1 to the resource manager.

    In Process Z, the resource manager performs the following algorithm: Try to select aOG from the gateway address list, so that the outside n-tuple (partly unspecified)(src:(aOB1,*); dest:(aOG,*); . . .) is not an outside n-tuple of an already existing partial gateway state. It's OK that the complete gateway state in the first row in box c already exists. This is because we can safely assume that node B1 will use a port number different from pB1 when sending traffic towards node A3.
26. The resource manager sends a request to the gateway to create the partial gateway state described on the third row in box d.
27. The gateway replies after creating the gateway state.
28. The resource manager sends a response including nA3, aOG.
29. The N/A sends a response including nA3, aOG to node B1.

    In process V, the gateway preferably starts a timer after creating a partial gateway state. When the timer reaches a certain value, gate lifetime, and the partial gateway state has not yet collapsed, the partial gateway state is deleted, releasing the gate.
30. The gateway informs the resource manager that the partial gateway state has been deleted. The resource manager updates its list of existing partial gateway states accordingly.

As mentioned above, in practical cases, it may happen that the reply in steps 8, 16, and 29 is cached. However, for this solution to work satisfactory, the cached data must be deemed invalid after a time interval which is smaller than the time distance between two consecutive flow initiations towards the same inside-realm node and port number.

Substitution Style—Destination Port Known

FIG. **11** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication through a substitution style gateway, using inside node (destination) port information for efficient multiplexation.

This applies when the port number pA that Node A is listening on becomes known to the N/A-translator in the name query. For example, the DNS query may have the form: "_port._protocol._MSISDN.operator.country". A specific example would be "_4712._tcp.070123456789.telia.se". Alternatively, the DNS query could have the form: "_service._protocol._MSISDN.operator.country". A specific example in this case would be "_http._tcp.0733634026.telia.se". The string "http" would then be translated into a port number, in this case **80**.

In the following example, the initial state is that a communication node A in the inside realm has started an application

that is listening for incoming traffic on port number pA. Node A has the name nA. Node A has registered itself in the inside realm so that the AAA-server has a profile which includes nA together with the network address aIA that is allocated to node A. A communication node B in the outside realm wishes to establish communication towards node A. Node B has knowledge of nA and pA.

In the following sequence, there are three inside nodes with names nA**1**, nA**2**, and nA**3**, inside-realm addresses aIA**1**, aIA**2**, and aIA**3**, listening to ports pA**1**, pA**2**, and pA**3**, respectively.

1. Node B sends a query including nA**1** and pA**1** to the N/A.
2. The N/A sends a request including nA**1** to the AAA-server.
3. The AAA-server looks up the network address, aIA**1**, corresponding to nA**1** and sends a reply including nA**1** and aIA**1** to the N/A.
4. The N/A sends a request including nA**1**, aIA**1**, and pA**1** to the gateway resource manager (GRM).
   In Process X, the resource manager performs the following algorithm: In this case it is assumed that there are no existing partial gateway states, also referred to as gates. The resource manager can therefore freely select aOG from the gateway address list.
5. The resource manager sends a request to the gateway to create the gateway state described in box a.
6. The gateway replies after creating the partial gateway state (gate).
7. The resource manager sends a response including aOG and pA**1**.
8. The N/A sends a response to node B including nA**1**, aOG, and pA**1**.
9. Node B sends a query including nA**2** and pA**2** to N/A.
10. The N/A sends a request including nA**2** to the AAA-server.
11. The AAA-server looks up the network address, aIA**2**, corresponding to nA**2** and sends a reply including nA**2** and aIA**2** to N/A.
12. The N/A sends a request including nA**2**, aIA**2**, and pA**2** to the resource manager.
    In Process Y, the resource manager performs the following algorithm: Try to select aOG from the gateway address list so that the outside n-tuple (partly unspecified)(src:(*,*); dest:(aOG, pA**2**); . . .) is not an outside n-tuple of an already existing partial gateway state. Assume in this example, that pA**2** is not equal pA**1**. This means that it's OK to select the same aOG as was selected in process X above. If pA**2** is equal to pA**1**, the resource manager should try to select an address from the gateway address list different from aOG.
13. The resource manager sends a request to the gateway to create the gateway state described on the second row in box b.
14. The gateway replies after creating the partial gateway state.
15. The resource manager sends a response including nA**2**, aOG, and pA**2**.
16. The N/A sends a response including nA**2**, aOG, and pA**2** to node B.
17. Node B sends the first packet in the communication flow towards node A**1**.
18. In the gateway, the partial gateway state collapses into a complete gateway state, whereby the outside n-tuple is completed so that it is: (src:(aOB, pB): dest:(aOG, pA**1**); . . .) and the inside n-tuple is (src:(aIA**1**, pA**1**); dest:(aOB, pB); . . .), as seen inbox c.
19. The packet is forwarded by the gateway towards node A**1**.
20. Node A**1** sends the next packet in the communication flow towards node B.
21. The packet is forwarded by the gateway towards node B.
22. Node B sends a query including nA**3** and pA**3** to N/A.
23. The N/A sends a request including nA**3** to the AAA-server.
24. The AAA-server looks up the network address, aIA**3**, corresponding to nA**3** and sends a reply including nA**3** and aIA**3** to N/A.
25. The N/A sends a request including nA**3**, aIA**3**, and pA**3** to the resource manager.
    In Process Z, the resource manager performs the following algorithm: Try to select aOG from the gateway address list so that the outside n-tuple (partly unspecified)(src:(*,*); dest:(aOG, pA**3**); . . .) is not an outside n-tuple of an already existing partial gateway state. It's OK that the complete gateway state in the first row in box c already exists. This is because we can safely assume that node B will use a port number different from pB when sending traffic towards node A**3**. If all addresses in the gateway address list are contained in existing partial gateway states together with the port number pA**3**, then the resource manager should select a new port number pG so that the outside n-tuple (partly unspecified)(src:(*,*); dest:(aOG, pG); . . .) is not an outside n-tuple of an already existing partial gateway state.
26. The gateway resource manager sends a request to the gateway to create the gateway state described on the third row in box d.
27. The gateway replies after creating the partial gateway state.
28. The resource manager sends a response including nA**3**, aOG, and pG.
29. The N/A sends a response including nA**3**, aOG, and pG to node B.
    In process V, the gateway starts a timer after creating a partial gateway state. When the timer reaches a certain value, and the partial state has not yet collapsed, the partial state is deleted.
30. The gateway informs the resource manager that the partial state has been deleted, and the resource manager updates its lists of existing partial gateway states accordingly.

As indicated in the sequence above, there are two cases. In the replies (steps 8, 16, and 29) from the N/A-translator, either the port number is equal to the port number sent in the respective queries (Steps 1, 9, and 22) or not. The former case is the desired since the application in node B is expecting to send towards port number pA. It is recommended that the latter case is used only as a fallback case since it may require implementation changes in the application in node B.

As before, cached data associated with replies back to an outside node must be handled with care.

Relaying Style—Source Address Known

FIG. **12** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication through a relaying style gateway, using outside node (source) address information for efficient multiplexation.

This solution applies when the network address of node B becomes known to the N/A-translator in the name query. This is the case if the name queries are delivered directly and not relayed by intermediate nodes. In the case when DNS is used for name look-up, this corresponds to disabling recursive look-ups, instead relying on iterative look-ups.

As previously mentioned, in the relaying case, the inside-realm node is aware of the outside-realm network address it

has been allocated. Thus, application software running on an inside-realm node expecting a communication flow initiated from the outside realm must bind to the currently assigned outside-realm network address. We can therefore assume that all inside nodes have been allocated outside-realm addresses. Since we must generally support more nodes than the number of outside-realm addresses that are available to the gateway, we must assume that some inside nodes are allocated the same outside-realm address. In the following sequence we show three inside nodes A1, A2, and A3, all having the same outside-realm address aOG. We furthermore assume that the gateway resource manager keeps track of which outside-realm address is allocated to a particular inside node based on some index represented in the sequence messages by the symbols "A1", "A2", and "A3". When the virtual point-to-point link toward an inside node is implemented as an IP-in-IP tunnel, an example would be that the symbol "A1" is the inside-realm address aIA1 allocated to the node A1.

1. Node B1 sends a query including nA1 to the N/A-translator. The address aOB1 is visible in the source field of the query packet.
2. The N/A-translator sends a request including nA1 to the AAA-server.
3. The AAA-server looks-up the symbol, A1, corresponding to nA1 and sends a reply including nA1 and A1 to the N/A.
4. The N/A sends a request including nA1, A1, and aOB1 to the gateway resource manager (GRM).

   In Process X, the gateway resource manager performs the following algorithm: In this case it is assumed that there are no existing partial gateway states, also referred to as gates. Based on the symbol A1, the resource manager finds aOG, the outside-realm address currently allocated to node A1.
5. The gateway resource manager sends a request to the gateway to create the gateway state described in box a.
6. The gateway replies after creating the gateway state.
7. The resource manager sends a response including nA1 and aOG.
8. The N/A sends a response including nA1 and aOG to node B1.
9. Node B2 sends a query including nA2 to N/A. The address aOB2 is visible in the source field of the query packet.
10. The N/A sends a request including nA2 to the AAA-server.
11. The AAA-server looks-up the symbol, A2, corresponding to nA2 and sends a reply including nA2 and A2 to the N/A.
12. The N/A sends a request including nA2, A2, and aOB2 to the gateway resource manager.

    In Process Y, the resource manager performs the following algorithm: Based on the symbol A2, the resource manager finds aOG, the outside-realm address currently allocated to node A2. If the outside n-tuple (partly unspecified) (src:(aOB2, *); dest:(aOG, *); . . .) is not an outside n-tuple of an already existing partial gateway state, then it's OK to create a new partial gateway state with that outside n-tuple. In this case, since aOB2 is not equal to aOB1, it's OK to create a new partial gateway state (gate), with the outside n-tuple (partly unspecified) (src:(aOB2, *); dest:(aOG, *); . . .).
13. The gateway resource manager sends a request to the gateway to create the gateway state described on the second row in box b.
14. The gateway replies after creating the partial gateway state.
15. The gateway resource manager sends a response including nA2 and aOG.
16. The N/A sends a response including nA2 and aOG to node B2.
17. Node B1 sends the first packet in the communication flow towards node A1.
18. In the gateway, the partial gateway state collapses into a complete gateway state, whereby the outside n-tuple is completed so that it is: (src:(aOB1, pB); dest:(aOG, pA1); . . .), as seen in box c.
19. The packet is forwarded by the gateway towards node A1 (relaying style).
20. Node A1 sends the next packet in the communication flow towards node B1.
21. The packet is forwarded by the gateway towards node B1 (relaying style).
22. Node B1 sends a query including nA3 to the N/A. The address aOB1 is visible in the source field of the query packet.
23. The N/A sends a request including nA3 to the AAA-server.
24. The AAA-server looks up the symbol, A3, corresponding to nA3 and sends a reply including nA3 and A3 to the N/A.
25. The N/A sends a request including nA3, A3, and aOB1 to the gateway resource manager.

    In Process Z, the resource manager performs the following algorithm: Based on the symbol A3, the resource manager finds aOG, the outside-realm address currently allocated to node A3. If the outside n-tuple (partly unspecified) (src:(aOB1, *); dest:(aOG, *); . . .) is not an outside n-tuple of an already existing partial gateway state (gate), then it's OK to create a new partial gateway state with that outside n-tuple. It's OK that the complete gateway state in the first row in box c already exists. This is because we can safely assume that node B1 will use a port number different from pB1 when sending traffic towards node A3. In case a partial gateway state with the outside n-tuple (partly unspecified)(src:(aOB1, *); dest:(aOG, *); . . .) already exists, then there is not enough information available to distinguish the soon incoming communication flows. Preferably, the resource manager should therefore instruct the N/A to either not respond at all towards node B2 or respond with an explicit error message. This error case is not shown in the sequence.
26. The gateway resource manager sends a request to the gateway to create the partial gateway state (gate) described on the third row in box d.
27. The gateway replies after creating the partial gateway state.
28. The resource manager sends a response including nA3 and aOG.
29. The N/A sends a response including nA3 and aOG to node B1.

    In process V, the gateway starts a timer after creating a partial gateway state. When the timer reaches a certain value, and the partial state has not yet collapsed, the state is deleted.
30. The gateway informs the gateway resource manager that the partial gateway state has been deleted, and the resource manager updates its lists of existing partial gateway states accordingly.

As before, cached data associated with replies back to an outside node must be handled with care.

Relaying Style Destination Port Known

FIG. **13** is a schematic sequence diagram illustrating the relevant signaling between the involved elements for an illustrative example of outside-realm initiated communication

through a relaying style gateway, using inside node (destination) port information for efficient multiplexation.

This applies when the port number pA that Node A is listening on becomes known to the N/A-translator in the name query.

In the following sequence we show three inside nodes A1, A2, and A3, all having the same outside-realm address aOG. Also, it is assumed that the gateway resource manager keeps track of which outside-realm address that is allocated to a particular inside node based on some index, represented in the sequence messages by the symbols "A1", "A2", and "A3".

1. Node B sends a query including nA1 and pA1 to the N/A.
2. The N/A sends a request including nA1 to the AAA-server.
3. The AAA-server looks-up the symbol, A1, corresponding to nA1 and sends a reply including nA1 and A1 to the N/A.
4. The N/A sends a request including nA1, A1, and pA1 to the gateway resource manager.

   In Process X, the resource manager performs the following algorithm: In this case it is assumed that there are no existing partial gateway states, also referred to as gates. Based on the symbol A1, the resource manager finds aOG, the outside-realm address currently allocated to node A1.
5. The gateway resource manager sends request to the gateway to create the gateway state described in box a.
6. The gateway replies after creating the partial gateway state.
7. The resource manager sends a response including nA1, aOG, and pA1.
8. The N/A sends a response including nA1, aOG, and pA1 to node B.
9. Node B sends a query including nA2 and pA2 to the N/A.
10. The N/A sends a request including nA2 to the AAA-server.
11. The AAA-server looks up the symbol, A2, corresponding to nA2 and sends a reply including nA2 and A2 to the N/A.
12. The N/A sends a request including nA2, A2, and pA2 to the gateway resource manager.

    In Process Y, the gateway resource manager performs the following algorithm:

    Based on the symbol A2, the resource manager finds aOG, the outside-realm address currently allocated to node A2. If the outside n-tuple (partly unspecified)(src:(*,*); dest:(aOG, pA2); . . .) is not an outside n-tuple of an already existing partial gateway state (gate), then it's OK to create a new partial gateway state with that outside n-tuple. In this case, this means that if pA2 is not equal pA1, then it's OK to create a new partial gateway state with the outside n-tuple (partly unspecified)(src:(*,*); dest:(aOG, pA2); . . .). On the other hand, if pA2 is equal to pA1 there is not enough information available to distinguish the soon incoming communication flows. The resource manager should therefore preferably instruct the N/A-translator to either not respond at all towards node B or respond with an explicit error message. This error case is not shown in the sequence.
13. The gateway resource manager sends a request to the gateway to create the gateway state described on the second row in box b.
14. The gateway replies after creating the partial gateway state (gate).
15. The resource manager sends a response including nA2, aOG, and pA2.
16. The N/A sends a response including nA2, aOG, and pA2 to node B.
17. Node B sends the first packet in the communication flow towards node A1.
18. In the gateway, the partial gateway state collapses into a complete gateway state, whereby the outside n-tuple is completed so that it is: (src:(aOB, pB); dest:(aOG, pA1); . . .), as seen in box c.
19. The packet is forwarded by the gateway towards node A1 (relaying style).
20. Node A1 sends the next packet in the communication flow towards node B.
21. The packet is forwarded by the gateway towards node B (relaying style).
22. Node B sends a query including nA3 and pA3 to the N/A.
23. The N/A sends a request including nA3 to the AAA-server.
24. The AAA-server looks-up the symbol, A3, corresponding to nA3 and sends a reply including nA3 and A3 to the N/A.
25. The N/A sends a request including nA3, A3, and pA3 to the resource manager.

    In Process Z, the resource manager performs the following algorithm: Based on the symbol A3, the resource manager finds aOG, the outside-realm address currently allocated to node A3. If the outside n-tuple (partly unspecified) (src:(*,*); dest:(aOG, pA3); . . .) is not an outside n-tuple of an already existing partial gateway state (gate), then it's OK to create a new partial gateway state with that outside n-tuple. If this is not possible we have the same error case as in Process Y above. It's OK that the complete gateway state in the first row in box c already exists. This is because we can safely assume that node B will use a port number different from pB when sending traffic towards node A3.
26. The gateway resource manager sends request to the gateway to create the gateway state described on the third row of box d.
27. The gateway replies after creating the partial gateway state.
28. The gateway resource manager sends a response including nA3, aOG, and pG.
29. The N/A sends a response including nA3, aOG, and pG to node B.

    In process V, the gateway starts a timer after creating a partial gateway state. When the timer reaches a certain value, and the gate has not yet collapsed, the gate is deleted.
30. The gateway informs the resource manager that the gate has been deleted, and the resource manager updates its lists of existing gates accordingly.

Implementation Examples

FIG. **14** is a schematic block diagram illustrating an implementation example of a system for providing connectivity between nodes of different address realms according to a particular embodiment of the invention. The implementation of FIG. **14** generally corresponds to the overall system overview of FIG. **9**, but with the gateway **30** and gateway resource manager **40** implemented in a modified firewall/network address translator (FW/NAT) node, and the N/A-translator implemented in a modified DNS-server. This means that the gateway resource manager **40** is co-located with the gateway **30**, and perhaps even integrated in the gateway.

FIG. **15** is a schematic block diagram illustrating an implementation example of a system for providing connectivity between nodes of different address realms according to another particular embodiment of the invention. In this example, the gateway resource manager **40** and the N/A-translator **50** are implemented in a modified DNS-server, whereas the gateway **30** is implemented in a modified FW/NAT node.

In yet another implementation, the gateway resource manager **40** is implemented in a separate network node.

The embodiments described above are merely given as examples, and it should be understood that the present invention is not limited thereto. Further modifications, changes and improvements which retain the basic underlying principles disclosed and claimed herein are within the scope of the invention.

REFERENCES

[1] *IP Network Address Translator (NAT) Terminology and Considerations*, P. Srisuresh, M. Holdrege, RFC 2663 of the Internet Engineering Task Force, August 1999.

[2] *Realm Specific IP: Framework*, M. Borella, J. Lo, D. Grabelsky, G. Montenegro, RFC 3102 of the Internet Engineering Task Force, October 2001.

[3] *Realm Specific IP: Protocol Specification*, M. Borella, D. Grabelsky, J. Lo, K. Taniguchi, RFC 3103 of the Internet Engineering Task Force, October 2001.

[4] http://www.permeo.com/pdf/solutionpaper1.pdf, 2002.

[5] *Address Allocation for Private Internets*, Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, RFC 1918 of the Internet Engineering Task Force, February 1996.

[6] *SIP: Session Initiation Protocol*, M. Handley, H. Schuilzrinne, E. Schooler, J. Rosenberg, RFC 2543 of the Internet Engineering Task Force, March 1999 2001.

The invention claimed is:

1. A method for supporting establishment of a requested connection between a node of an inside address realm and a node of an outside address realm through an intermediate communication gateway having a gateway address pool comprising a limited number of available ontside-realm gateway addresses for enabling outside-realm representation of inside-realm nodes, said method comprising the steps of:

i) providing multiplexing information including at least one of network address information and port information of at least one of said inside-realm node and said outside-realm node;

ii) performing, prior to initiating establishment of said requested connection, a network address allocation procedure to determine an outside-realm gateway address based on a unique combination of one of said limited number of outside-realm gateway addresses and said multiplexing information, said network address allocation procedure including the steps of:

selecting, from said gateway address pool, a candidate outside-realm gateway address for combination with said multiplexing information,

determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection;

repeating, if the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection, the selecting step until a unique combination is found that is not already being utilized for another connection,

wherein the unique combination of outside-realm gateway address and said multiplexing information defines an outside-realm gateway state representation that has no counterpart in a predetermined set of existing gateway connection states, and said determining step is based on a comparison in relation to said predetermined set of existing gateway connection states,

wherein said multiplexing information, for an inside-realm initiated connection, includes at least one of outside node address information and outside node port information, said outside-realm gateway state representation is an at least partially complete gateway state representation, and said predetermined set of gateway connection states includes the existing gateway connection states in said gateway; and

iii) thereafter, initiating establishment of said requested connection based on the unique combination of outside-realm gateway address and said multiplexing information.

2. The method according to claim **1**, further comprising the step of maintaining a separate list representation of said predetermined set of existing gateway connection states, and wherein said outside-realm gateway state representation is selected based on comparison with corresponding information of said gateway connection states represented in said list representation.

3. The method according to claim **1**, wherein said selecting step also includes selecting associated gateway port information for combination with said multiplexing information, said outside-realm representation is a complete outside-realm representation, and said step of initiating establishment of said connection comprises the step of reqnesting that said gateway creates a gateway connection state based on said complete outside-realm representation.

4. The method according to claim **1**, wherein said outside-realm representation is a partially complete outside-realm representation, and said step of initiating establishment of said connection comprises the step of requesting that said gateway creates a partially complete gateway connection state based on said partially complete outside-realm representation.

5. A method for supporting establishment of a requested connection between a node of an inside address realm and a node of an outside address realm through an intermediate communication gateway having a gateway address pool comprising a limited number of available outside-realm gateway addresses for enabling outside-realm representation of inside-realm nodes, said method comprising the steps of:

i) providing multiplexing information including at least one of network address information and port information of at least one of said inside-realm node and said outside-realm node;

ii) performing, prior to initiating establishment of said requested connection, a network address allocation procedure to determine an outside-realm gateway address based on a unique combination of one of said limited number of outside-realm gateway addresses and said multiplexing information, said network address allocation procedure including the steps of:

selecting, from said gateway address pool, a candidate outside-realm gateway address for combination with said multiplexing information,

determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection;

repeating, if the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection, the selecting step until a unique combination is found that is not already being utilized for another connection,

wherein the unique combination of outside-realm gateway address and said multiplexing information defines an outside-realm gateway state representation that has no counterpart in a predetermined set of existing gateway

connection states, and said determining step is based on a comparison in relation to said predetermined set of existing gateway connection states,

wherein said multiplexing information, for an outside-realm initiated connection, includes at least one of outside node address information and inside node port information, said outside-realm gateway state representation is a partially complete gateway state representation and said predetermined set of gateway connection states includes the existing partially complete gateway connection states in said gateway; and

iii) thereafter, initiating establishment of said requested connection based on the unique combination of outside-realm gateway address and said multiplexing information.

6. The method according to claim **5**, wherein outside-realm gateway addresses of the gateway are traversed until finding an outside-realm gateway address, which in combination with said multiplexing information has no counterpart in any existing partially complete gateway connection state.

7. The method according to claim **5**, wherein said step of determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for a connection comprises the step of verifying that a pre-allocated outside-realm gateway address in combination with said

multiplexing information has no counterpart in any existing partially complete gateway connection state.

8. The method according to claim **5**, wherein said step of initiating establishment of said connection comprises the step of requesting that said gateway establishes a partially complete gateway connection state based on said partially complete outside-realm representation.

9. The method according to claim **8**, further comprising the step of transforming, upon receipt of a packet from said outside node to said gateway, said partially complete gateway connection state that has been created in said gateway into a complete gateway connection state based on complementary connection information associated with said packet.

10. The method according to claim **9**, wherein said multiplexing information is predetermined outside node address information, and said complementary connection information includes inside node port information and outside node port information.

11. The method according to claim **9**, wherein said multiplexing information is predetermined inside node port information, and said complementary connection information includes outside node address information and outside node port information.

12. The method according to claim **5**, further comprising the steps of:

selecting, if it is not possible to find a unique combination based on predetermined inside node port information, another gateway port; and

selecting an outside-realm gateway address based on said selected gateway port to define a unique, partially complete outside-realm representation of a gateway connection state.

13. The method according to claim **5**, wherein said multiplexing information originates from a user-resource identifier query initiated from said outside node.

14. The method according to claim **5**, wherein said connection establishment is based on said outside-realm gateway state representation and a corresponding inside-realm gateway state representation.

15. The method according to claim **5**, further comprising the steps of:

preparing, at said outside node, a user-resource identifier query that includes an inside node identifier as well as said multiplexing information including at least one of outside node address information and inside node port information;

determining inside-realm network address information based on said inside node identifier included in said identifier query; selecting, based on said multiplexing information included in said identifier query, said outside-realm gateway address to be used in establishing a dynamic gateway

connection state for a flow between said outside node and said inside node through said gateway; and

establishing said dynamic gateway connection state based on said selected outside-realm gateway address, said multiplexing information included in said identifier query and said inside-realm network address information, thereby enabling an outside-realm initiated connection.

16. The method according to claim **15**, wherein said step of establishing said dynamic gateway connection state comprises the steps of:

creating a partially complete gateway connection state based on said selected outside-realm gateway address, said multiplexing information included in said identifier query and said inside-realm network address information; and

upon receipt of a packet from said outside node to said gateway, transforming said partially complete gateway state into a complete gateway connection state based on complementary connection information associated with said packet.

17. The method according to claim **16**, wherein said multiplexing information included in said identifier query is an outside network address of said outside node, and said complementary connection information for completing the gateway connection state includes a port number of said inside node and a port number of said outside node.

18. The method according to claim **16**, wherein said multiplexing information included in said identifier query is an inside node port number, and said complementary connection information for completing the gateway connection state

includes an outside network address of said outside node and a port number of said outside node.

19. The method according to claim **15**, wherein said step of selecting an outside-realm gateway address comprises the step of selecting an outside-realm gateway address, which in combination with said multiplexing information included in said identifier-query defines a partially complete outside-realm gateway state representation that has no counterpart in any existing partially complete gateway connection state.

20. The method according to claim **19**, further comprising the step of maintaining a separate list representation of existing partially complete gateway connection states, and wherein said partially complete outside-realm representation is

allocated based on comparison with corresponding information of all existing partially complete gateway connection states represented in said list representation.

21. The method according to claim **20**, wherein outside-realm gateway addresses associated with said gateway are traversed until finding an outside-realm gateway address, which in combination with said multiplexing information included in said identifier query has no counterpart in any existing partially complete gateway connection state represented in said list representation.

22. The method according to claim 20, wherein said step of determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for a connection comprises the step of verifying that a pre-allocated outside-realm gateway address in combination with said multiplexing information included in said identifier query has no counterpart in any existing partially complete gateway connection state represented in said list representation.

23. The method according to claim 15, further comprising the step of notifying said outside node of said selected outside-realm gateway address.

24. The method according to claim 15, wherein said user-resource identifier query is a Domain Name Server (DNS) query.

25. The method according to claim 15, wherein said inside address realm is a private address realm and said outside address realm is a public address realm.

26. A device for supporting establishment of a requested connection between a node of an inside address realm and a node of an outside address realm through an intermediate communication gateway having a gateway address pool comprising a limited number of available outside-realm gateway addresses for enabling outside-realm representation of inside-realm nodes, said device comprising:

i) means for providing multiplexing information including at least one of network address information and port information of at least one of said inside-realm node and said outside-realm node;

ii) means for network address allocation to determine an outside-realm gateway address based on a unique combination of one of said limited number of outside-realm gateway addresses and said multiplexing information, said network address allocation means being configured, prior to initiating establishment of said requested connection, for:

selecting, from said gateway address pool, a candidate outside-realm gateway address for combination with said multiplexing information,

determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection;

repeating, if the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection, the selection of outside-realm gateway address until a unique combination is found that is not already being utilized for another connection,

wherein the unique combination of outside-realm gateway address and said multiplexing information defines an outside-realm gateway state representation that has no counterpart in a predetermined set of existing gateway connection states, and said network address allocation means is configured for determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection based on a comparison in relation to said predetermined set of existing gateway connection states,

wherein said multiplexing information, for an inside-realm initiated connection, includes at least one of outside node address information and outside node port information, said outside-realm gateway state representation is an at least partially complete gateway state representation, and said predetermined set of gateway connection states includes the existing gateway connection states in said gateway; and

iii) means for initiating establishment of said requested connection based on the unique combination of outside-realm gateway address and said multiplexing information.

27. The device according to claim 26, further comprising means for maintaining a separate list representation of said predetermined set of existing gateway connection states, and wherein said network address allocation means is configured for finding said outside-realm gateway state representation based on comparison with corresponding information of said gateway connection states represented in said list representation.

28. The device according to claim 26, wherein said network address allocation means is configured for selecting also associated gateway port information for combination with said multiplexing information, said outside-realm representation is a complete outside-realm representation, and said means for initiating establishment of said connection comprises means for requesting that said gateway creates a gateway connection state based on said complete outside-realm representation.

29. The device according to claim 26, wherein said outside-realm representation is a partially complete outside-realm representation, and said means for initiating establishment of said connection comprises means for requesting that said gateway creates a partially complete gateway connection state based on said partially complete outside-realm representation.

30. A device for supporting establishment of a requested connection between a node of an inside address realm and a node of an outside address realm through an intermediate communication gateway having a gateway address pool comprising a limited number of available outside-realm gateway addresses for enabling outside-realm representation of inside-realm nodes, said device comprising:

i) means for providing multiplexing information including at least one of network address information and port information of at least one of said inside-realm node and said outside-realm node;

ii) means for network address allocation to determine an outside-realm gateway address based on a unique combination of one of said limited number of outside-realm gateway addresses and said multiplexing information, said network address allocation means being configured, prior to initiating establishment of said requested connection, for:

selecting, from said gateway address pool, a candidate outside-realm gateway address for combination with said multiplexing information,

determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection;

repeating, if the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection, the selection of outside-realm gateway address until a unique combination is found that is not already being utilized for another connection,

wherein the unique combination of outside-realm gateway address and said multiplexing information defines an outside-realm gateway state representation that has no counterpart in a predetermined set of existing gateway connection states, and said network address allocation

means is configured for determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection based on a comparison in relation to said predetermined set of existing gateway connection states,

wherein said multiplexing information, for an outside-realm initiated connection, includes at least one of outside node address information and inside node port information, said outside-realm gateway state representation is a partially complete gateway state representation and said predetermined set of gateway connection states includes the existing partially complete gateway connection states in said gateway; and

iii) means for initiating establishment of said requested connection based on the unique combination of outside-realm gateway address and said multiplexing information.

31. The device according to claim **30**, wherein said network address allocation means is configured for traversing outside-realm gateway addresses of the gateway until finding an outside-realm gateway address, which in combination with said multiplexing information has no counterpart in any existing partially complete gateway connection state.

32. The device according to claim **30**, wherein said means for determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for a connection comprises means for verifying that a pre-allocated outside-realm gateway address in combination with said multiplexing information has no counterpart in any existing partially complete gateway connection state.

33. The device according to claim **30**, wherein said means for initiating establishment of said connection comprises means for requesting that said gateway establishes a partially complete gateway connection state based on said partially complete outside-realm representation.

34. The device according to claim **33**, further comprising means for transforming, upon receipt of a packet from said outside node to said gateway, said partially complete gateway connection state that has been created in said gateway into a complete gateway connection state based on complementary connection information associated with said packet.

35. The device according to claim **34**, wherein said multiplexing information is predetermined outside node address information, and said complementary connection information includes inside node port information and outside node port information.

36. The device according to claim **34**, wherein said multiplexing information is predetermined inside node port information, and said complementary connection information includes outside node address information and outside node port information.

37. The device according to claim **30**, further comprising means for selecting, if it is not possible to find a unique combination based on predetermined inside node port information, another gateway port, and means for selecting an

outside-realm gateway address based on said selected gateway port to define a unique, partially complete outside-realm representation of a gateway connection state.

38. The device according to claim **30**, wherein said multiplexing information originates from a user-resource identifier query initiated from said outside node.

39. The device according to claim **30**, wherein said means for initiating establishment of said connection is configured to operate based on said outside-realm gateway state representation and a corresponding inside-realm gateway state representation.

40. The device according to claim **30**, further comprising:

means, responsive to a user-resource identifier query from said outside node, for determining inside-realm network address information based on an inside node identifier included in said identifier query, wherein said identifier query further includes said multiplexing information including at least one of outside node address information and inside node port information;

means for selecting, based on said multiplexing information included in said identifier query, said outside-realm gateway address to be used in establishing a dynamic gateway connection state for a flow between said outside node and said inside node through said gateway; and

means for establishing said dynamic gateway connection state based on said selected outside-realm gateway address, said multiplexing information included in said identifier query and said inside-realm network address information, thereby enabling an outside-realm initiated connection.

41. The device according to claim **40**, wherein said means for establishing said dynamic gateway connection state comprises:

means for creating a partially complete gateway connection state based on said selected outside-realm gateway address, said multiplexing information included in said identifier query and said inside-realm network address information; and

means for transforming, upon receipt of a packet from said outside node to said gateway, said partially complete gateway state into a complete gateway connection state based on complementary connection information associated with said packet.

42. The device according to claim **41**, wherein said multiplexing information included in said identifier query is an outside network address of said outside node, and said complementary connection information for completing the gateway connection state includes a port number of said inside node and a port number of said outside node.

43. The device according to claim **41**, wherein said multiplexing information included in said identifier query is an inside node port number, and said complementary connection information for completing the gateway connection state includes an outside network address of said outside node and a port number of said outside node.

44. The device according to claim **40**, wherein said means for selecting an outside-realm gateway address is operable for selecting an outside-realm gateway address, which in combination with said multiplexing information included in said identifier-query defines a partially complete outside-realm gateway state representation that has no counterpart in any existing partially complete gateway connection state.

45. The device according to claim **44**, further comprising means for maintaining a separate list representation of existing partially complete gateway connection states, and wherein said network address allocation means is configured for finding said partially complete outside-realm representation based on comparison with corresponding information of all existing partially complete gateway connection states represented in said list representation.

46. The device according to claim **45**, wherein said network address allocation means is configured for traversing outside-realm gateway addresses associated with said gateway until finding an outside-realm gateway address, which in

combination with said multiplexing information included in said identifier query has no counterpart in any existing partially complete gateway connection state represented in said list representation.

47. The device according to claim **45**, wherein said means for determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for a connection comprises means for verifying that a pre-allocated outside-realm gateway address in combination with said multiplexing information included in said identifier query has no counterpart in any existing partially complete gateway connection state represented in said list representation.

48. The device according to claim **40**, further comprising means for notifying said outside node of said selected outside-realm gateway address.

49. The device according to claim **40**, wherein said user-resource identifier query is a Domain Name Server (DNS) query.

50. The device according to claim **40**, wherein said inside address realm is a private address realm and said outside address realm is a public address realm.

51. A gateway resource manager for a communication gateway that has a limited number of available outside-realm gateway addresses for enabling outside-realm representation of inside-realm nodes, said gateway resource manager comprising:

i) an input configured to receive multiplexing information including at least one of network address information and port information of at least one of said inside-realm node and said outside-realm node;

ii) network address allocation circuitry configured to determine an outside-realm gateway address based on a unique combination of one of said limited number of outside-realm gateway addresses and said multiplexing information, said network address allocation circuitry being configured to perform the following tasks prior to initiating establishment of a requested connection:

select, from said outside-realm gateway addresses, a candidate outside-realm gateway address for combination with said multiplexing information;

determine whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection;

repeat, if the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection, the selection of outside-realm gateway address until a unique combination is found that is not already being utilized for another connection,

wherein the unique combination of outside-realm gateway address and said multiplexing information defines an outside-realm gateway state representation that has no counterpart in a predetermined set of existing gateway connection states, and said network address allocation circuitry is configured for determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection based on a comparison in relation to said predetermined set of existing gateway connection states,

wherein said multiplexing information, for an inside-realm initiated connection, includes at least one of outside node address information and outside node port information, said outside-realm gateway state representation is an at least partially complete gateway state representation, and said predetermined set of gateway connection states includes the existing gateway connection states in said gateway; and

iii) resource allocation circuitry configured to initiate establishment of said requested connection based on the unique combination of outside-realm gateway address and said multiplexing information.

52. The gateway resource manager according to claim **51**, wherein said network address allocation circuitry is configured for finding said outside-realm gateway state representation based on comparison with corresponding information of said gateway connection states represented in a list representation of said predetermined set of existing gateway connection states.

53. A gateway resource manager for a communication gateway that has a limited number of available outside-realm gateway addresses for enabling outside-realm representation of inside-realm nodes, said gateway resource manager comprising:

i) an input configured to receive multiplexing information including at least one of network address information and port information of at least one of said inside-realm node and said outside-realm node;

ii) network address allocation circuitry configured to determine an outside-realm gateway address based on a unique combination of one of said limited number of outside-realm gateway addresses and said multiplexing information, said network address allocation circuitry being configured to perform the following tasks prior to initiating establishment of a requested connection:

select, from said outside-realm gateway addresses, a candidate outside-realm gateway address for combination with said multiplexing information;

determine whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection;

repeat, if the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection, the selection of outside-realm gateway address until a unique combination is found that is not already being utilized for another connection,

wherein the unique combination of outside-realm gateway address and said multiplexing information defines an outside-realm gateway state representation that has no counterpart in a predetermined set of existing gateway connection states, and said network address allocation circuitry is configured for determining whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for another connection based on a comparison in relation to said predetermined set of existing gateway connection states,

wherein said multiplexing information, for an outside-realm initiated connection, includes at least one of outside node address information and inside node port information, said outside-realm gateway state representation is a partially complete gateway state representation and said predetermined set of gateway connection states includes the existing partially complete gateway connection states in said gateway; and

iii) resource allocation circuitry configured to initiate establishment of said requested connection based on the unique combination of outside-realm gateway address and said multiplexing information.

54. The gateway resource manager according to claim **53**, wherein said input is configured to receive inside-realm net-

work address information corresponding to an inside node, and multiplexing information including at least one of outside node address information and inside node port information:

said outside-realm gateway address is to be used in establishing a dynamic gateway connection state for a flow between said outside node and said inside node through said gateway;

said resource allocation circuitry is configured to request said gateway to establish said dynamic gateway connection state based on said selected outside-realm gateway address, said multiplexing information and said inside-realm network address information.

55. The gateway resource manager according to claim **54**, wherein said multiplexing information is an outside node address, and said input is configured to request allocation of said selected outside-realm gateway address to said inside node for traffic coming from said outside node address.

56. The gateway resource manager according to claim **54**, wherein said input is configured to send a request to said gateway for establishment of a partially complete gateway connection state based on said selected outside-realm gateway address, said multiplexing information and said inside-realm network address information.

57. The gateway resource manager according to claim **56**, further comprising: means for receiving a reply from said gateway that said partially complete gateway connection state has been created; and

means for notifying said outside node of said selected outside-realm gateway address in response to said reply from said gateway.

58. The gateway resource manager according to claim **56**, wherein said network address allocation circuitry is configured to select an outside-realm gateway address, which in combination with said multiplexing information, defines a partially complete outside-realm gateway state representation that has no counterpart in any existing partially complete gateway connection state.

59. The gateway resource manager according to claim **58**, further comprising means for maintaining a list representation of existing partially complete gateway connection states, and wherein said network address allocation circuitry is configured to find said partially complete outside-realm representation based on comparison with corresponding information of all existing partially complete gateway connection states represented in said list representation.

60. The gateway resource manager according to claim **53**, wherein said network address allocation circuitry is configured to determine whether the combination of the selected candidate outside-realm gateway address and said multiplexing information is already being utilized for a connection based on comparison with established connections and/or connections under establishment.

* * * * *

EXHIBIT 1008

U.S. Patent No. 7,290,060 to *Kong* ("*Kong*")

US007290060B2

(12) **United States Patent**
Kong

(10) **Patent No.: US 7,290,060 B2**
(45) **Date of Patent: Oct. 30, 2007**

(54) **NETWORK-CONNECTING APPARATUS AND METHOD FOR PROVIDING DIRECT CONNECTIONS BETWEEN NETWORK DEVICES IN DIFFERENT PRIVATE NETWORKS**

(75) Inventor: **Won-keun Kong**, Suwon (KR)

(73) Assignee: **Samsung Electronics Co., Ltd.**, Suwon (KR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 812 days.

(21) Appl. No.: **10/379,674**

(22) Filed: **Mar. 6, 2003**

(65) **Prior Publication Data**

US 2003/0172184 A1 Sep. 11, 2003

(30) **Foreign Application Priority Data**

Mar. 7, 2002 (KR) 2002-0012219

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/245**; 709/249; 709/238; 370/352; 370/389

(58) **Field of Classification Search** 709/245, 709/203, 217, 238, 250, 225–226, 249; 370/352, 370/389
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,777,989	A *	7/1998	McGarvey	370/254
6,393,488	B1	5/2002	Araujo	
6,445,922	B1 *	9/2002	Hiller et al.	709/238
6,515,974	B1 *	2/2003	Inoue et al.	370/352
6,523,068	B1 *	2/2003	Beser et al.	709/245
6,708,219	B1 *	3/2004	Borella et al.	709/245
6,781,982	B1 *	8/2004	Borella et al.	370/352
6,801,523	B1 *	10/2004	Osman	370/352
6,810,417	B2 *	10/2004	Lee	709/238
6,948,003	B1 *	9/2005	Newman et al.	709/250
6,967,954	B2 *	11/2005	Sugiyama	370/395.52
7,072,323	B2 *	7/2006	Roberts et al.	370/338
2002/0026528	A1 *	2/2002	Lo	709/245
2002/0061011	A1 *	5/2002	Wan	370/352
2002/0067731	A1 *	6/2002	Houston et al.	370/401
2002/0101859	A1 *	8/2002	Maclean	370/352
2002/0103931	A1 *	8/2002	Mott	709/245

(Continued)

FOREIGN PATENT DOCUMENTS

JP 11-112577 A 4/1999

(Continued)

OTHER PUBLICATIONS

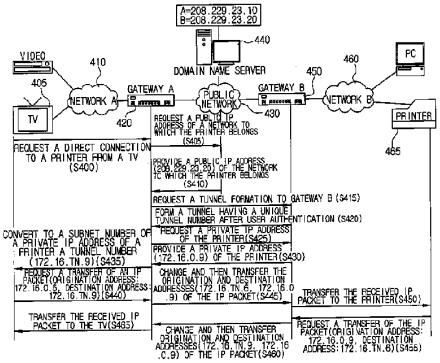
Launois De C et al.: Connection of Extruded Subnets: A Solution Based on RSIP:, IEEE Communications Magazine, IEEE Service Center, Piscataway, N.J, US, vol. 40, No. 9, Sep. 2002, pp. 116-121, XP001124128.

Primary Examiner—Philip Tran
(74) *Attorney, Agent, or Firm*—Sughrue Mion Pllc.

(57) **ABSTRACT**

A network-connecting apparatus for a first private network having a first network device. The apparatus includes a direct connection part for providing a direct connection in response to a connection request from the first network device, said request being a request to connect to a second network device in a second private network. Further, an address change part is provided for changing subnet numbers of origination and destination addresses of a packet transferred outside the first private network through the direct connection.

8 Claims, 5 Drawing Sheets



U.S. PATENT DOCUMENTS

2002/0133534 A1*	9/2002	Forslow	709/223
2003/0048804 A1*	3/2003	Inouchi et al.	370/466
2003/0112808 A1*	6/2003	Solomon	370/395.52
2003/0154306 A1*	8/2003	Perry	709/245

FOREIGN PATENT DOCUMENTS

JP	2000-228674 A	8/2000

* cited by examiner

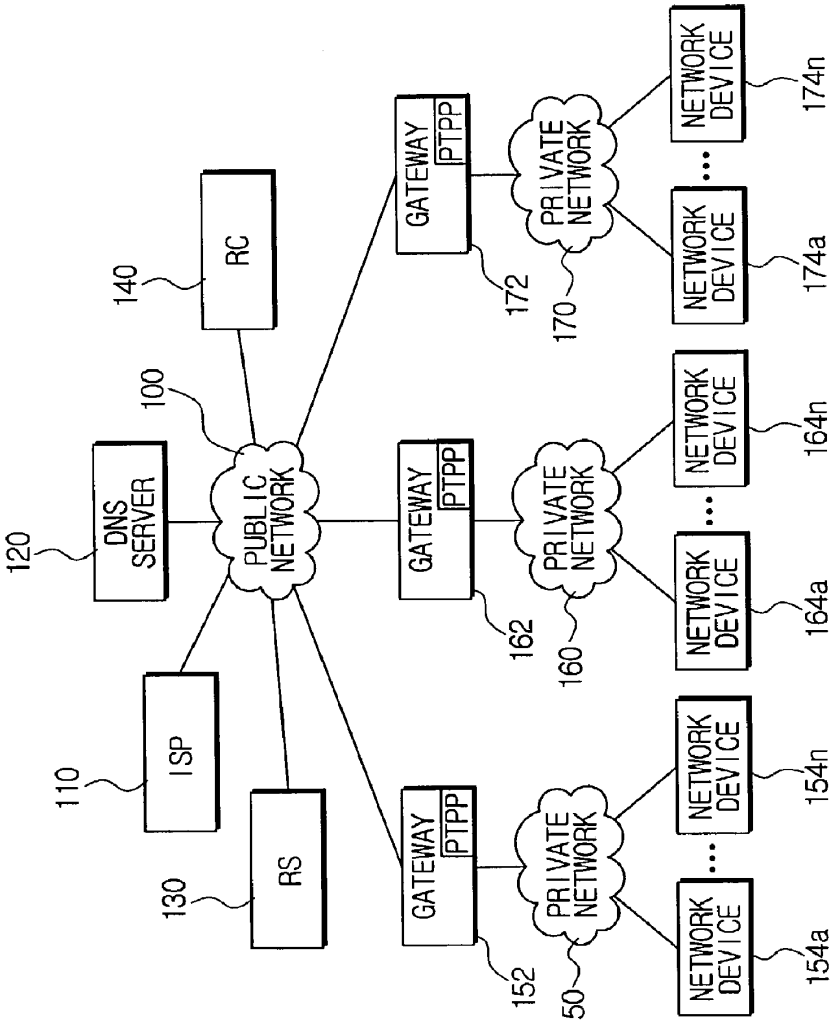

RC
140
GATEWAY
PTPP
172
PRIVATE NETWORK
170
NETWORK DEVICE
174n
NETWORK DEVICE
174a
100
DNS SERVER
120
PUBLIC NETWORK
GATEWAY
PTPP
162
PRIVATE NETWORK
160
NETWORK DEVICE
164n
NETWORK DEVICE
164a
ISP
110
RS
130
GATEWAY
PTPP
152
PRIVATE NETWORK
150
NETWORK DEVICE
154n
NETWORK DEVICE
154a

FIG. 1

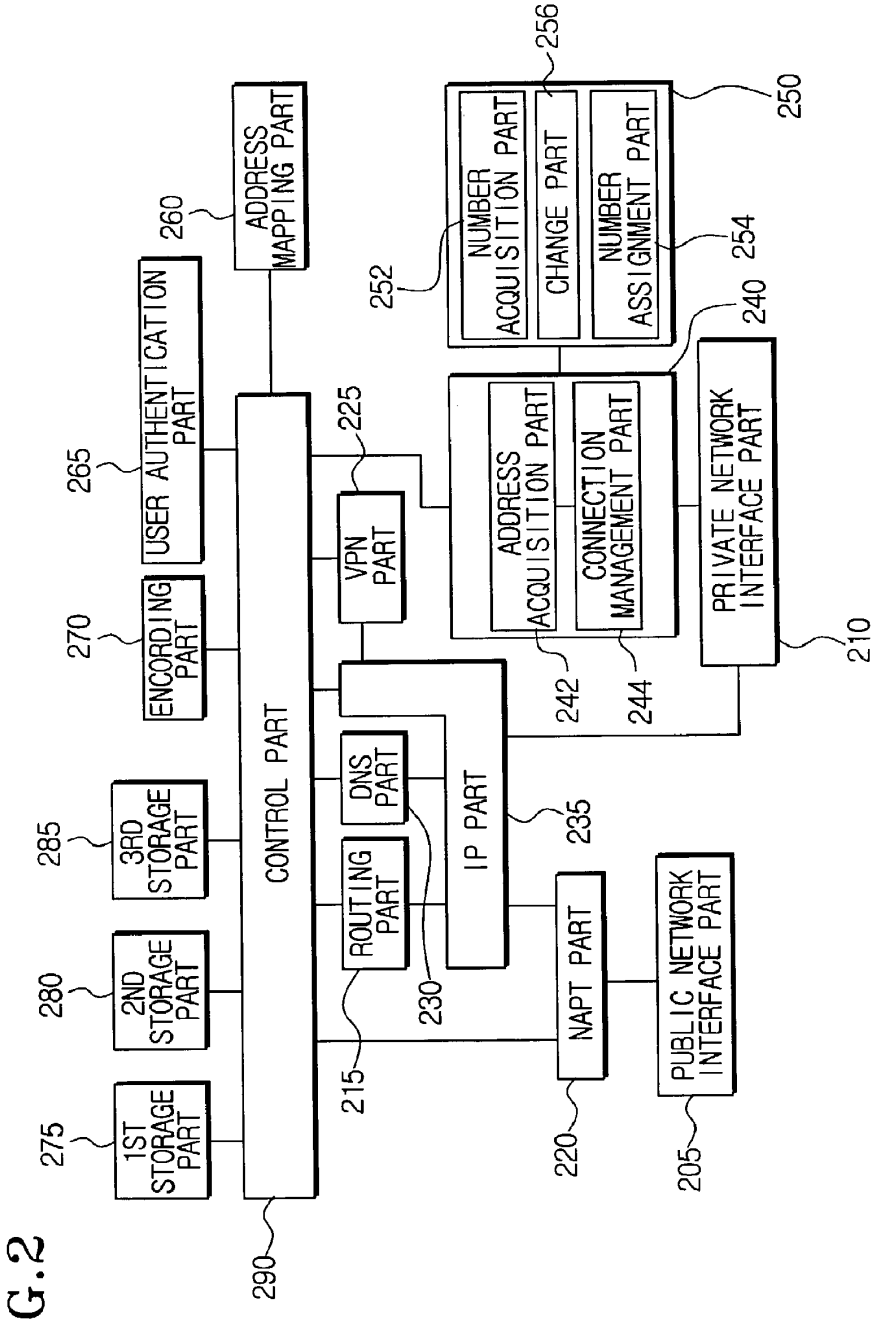
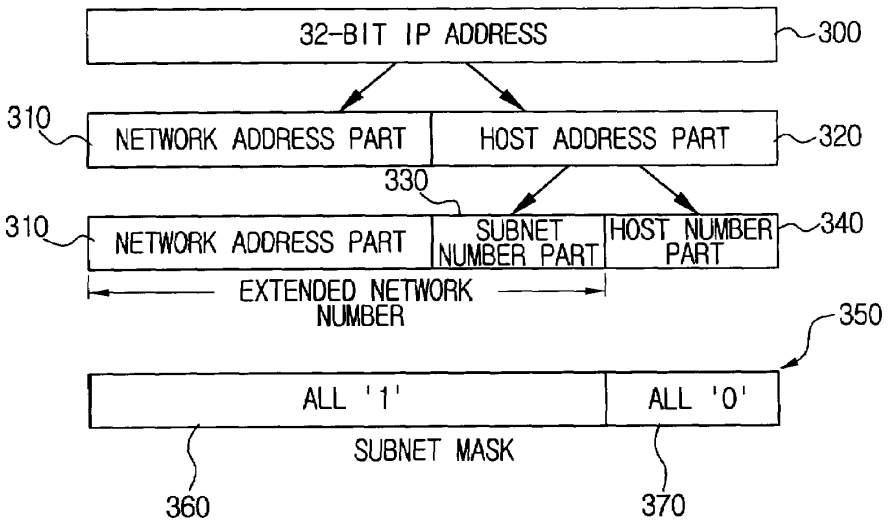

256
250
NUMBER ACQUISITION PART
CHANGE PART
NUMBER ASSIGNMENT PART
252
254
240
ADDRESS MAPPING PART
260
USER AUTHENTICATION PART
265
ADDRESS ACQUISITION PART
CONNECTION MANAGEMENT PART
PRIVATE NETWORK INTERFACE PART
225
VPN PART
270
ENCORDING PART
CONTROL PART
242
244
210
DNS PART
IP PART
235
285
3RD STORAGE PART
ROUTING PART
280
2ND STORAGE PART
230
NAPT PART
PUBLIC NETWORK INTERFACE PART
215
275
1ST STORAGE PART
220
205
290

FIG.2

FIG.3


32-BIT IP ADDRESS
300
310
NETWORK ADDRESS PART
HOST ADDRESS PART
320
330
310
NETWORK ADDRESS PART
SUBNET NUMBER PART
HOST NUMBER PART
340
EXTENDED NETWORK NUMBER
350
ALL '1'
ALL '0'
SUBNET MASK
360
370

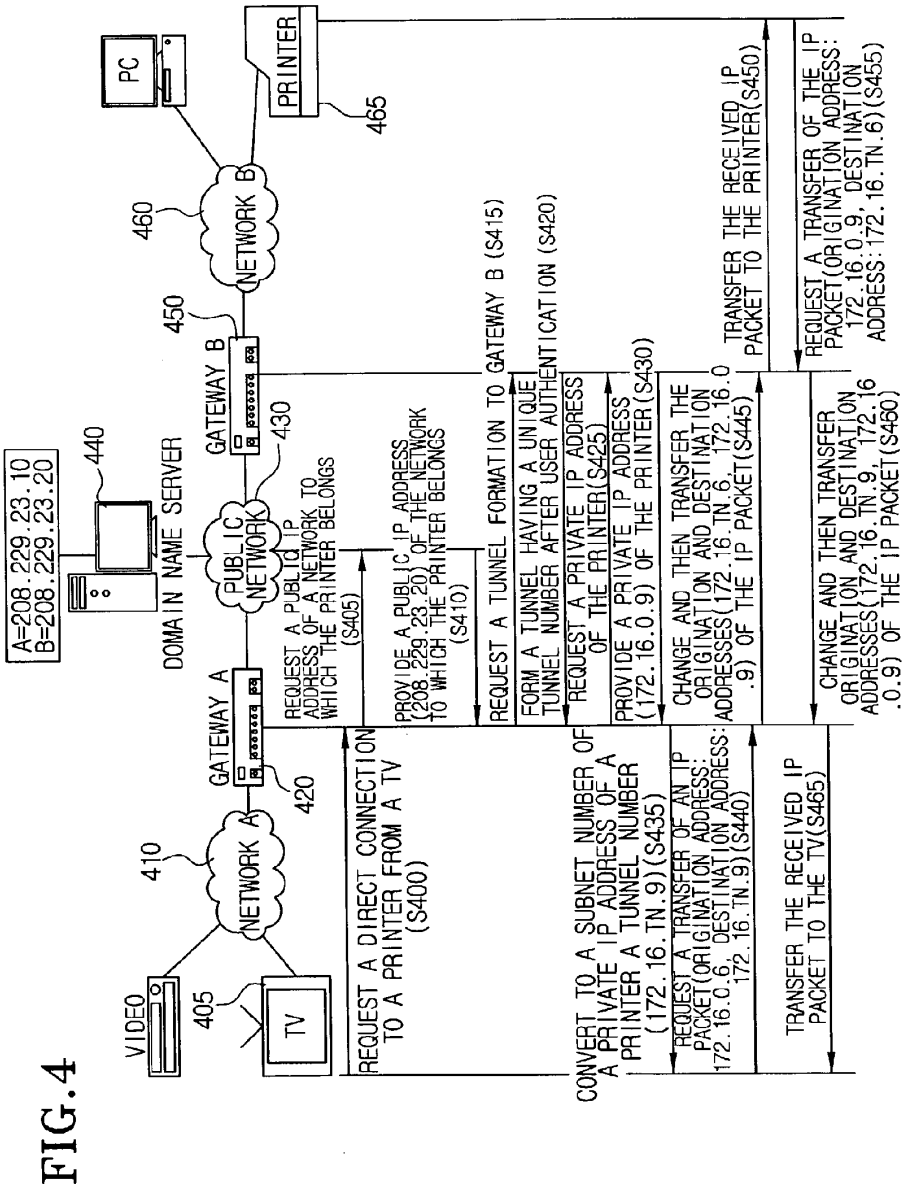
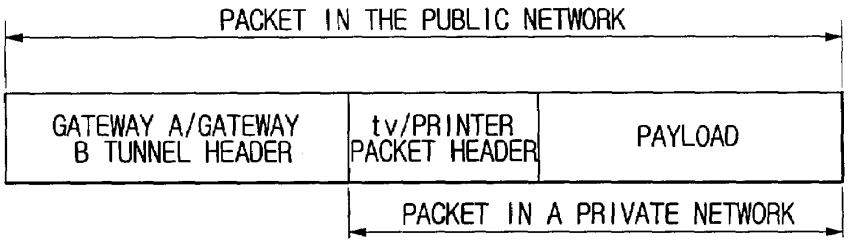

A=208.229.23.10
B=208.229.23.20
440
DOMAIN NAME SERVER
PC
PRINTER
465
460
NETWORK B
450
GATEWAY B
430
PUBLIC NETWORK
REQUEST A PUBLIC IP ADDRESS OF A NETWORK TO WHICH THE PRINTER BELONGS (S405)
PROVIDE A PUBLIC IP ADDRESS (208.229.23.20) OF THE NETWORK TO WHICH THE PRINTER BELONGS (S410)
REQUEST A TUNNEL FORMATION TO GATEWAY B (S415)
FORM A TUNNEL HAVING A UNIQUE TUNNEL NUMBER AFTER USER AUTHENTICATION (S420)
REQUEST A PRIVATE IP ADDRESS OF THE PRINTER(S425)
PROVIDE A PRIVATE IP ADDRESS (172.16.0.9) OF THE PRINTER(S430)
CHANGE AND THEN TRANSFER THE ORIGINATION AND DESTINATION ADDRESSES(172.16.TN.6, 172.16.0.9) OF THE IP PACKET(S445)
TRANSFER THE RECEIVED IP PACKET TO THE PRINTER(S450)
REQUEST A TRANSFER OF THE IP PACKET(ORIGINATION ADDRESS: 172.16.0.9, DESTINATION ADDRESS: 172.16.TN.6)(S455)
CHANGE AND THEN TRANSFER ORIGINATION AND DESTINATION ADDRESSES(172.16.TN.9, 172.16.0.9) OF THE IP PACKET(S460)
TRANSFER THE RECEIVED IP PACKET TO THE TV(S465)
REQUEST A TRANSFER OF AN IP PACKET(ORIGINATION ADDRESS: 172.16.C.6, DESTINATION ADDRESS: 172.16.TN.9)(S440)
CONVERT TO A SUBNET NUMBER OF A PRIVATE IP ADDRESS OF A PRINTER A TUNNEL NUMBER (172.16.TN.9)(S435)
REQUEST A DIRECT CONNECTION TO A PRINTER FROM A TV (S400)
GATEWAY A
420
NETWORK A
410
VIDEO
405
TV

FIG.4

FIG.5


PACKET IN THE PUBLIC NETWORK
GATEWAY A/GATEWAY B TUNNEL HEADER
tv/PRINTER PACKET HEADER
PAYLOAD
PACKET IN A PRIVATE NETWORK

NETWORK-CONNECTING APPARATUS AND METHOD FOR PROVIDING DIRECT CONNECTIONS BETWEEN NETWORK DEVICES IN DIFFERENT PRIVATE NETWORKS

BACKGROUND

This Application claims priority from Korean Patent Application No.2002-12219, the disclosure of which is incorporated herein by reference.

1. Field

This disclosure is related to a network-connecting apparatus and method. Specifically, techniques related to a network-connecting apparatus and method for providing direct connections between network devices in a first arbitrary private network and network devices in a second arbitrary private network are taught.

2. Description of the Related Art

A device for IP communication over the Internet requires an IP address that is unique and distinguishable from another device. The IP addresses that are presently allocated and used based on a code that is 32 bits long. However, with the increase in demand for devices to be hooked up to the Internet, a shortage of newly allocable IP addresses is anticipated. A scheme of using private IP addresses has been developed and employed to overcome this problem.

Private IP addresses are allocated on the condition that certain parts of the entire IP addresses can be used for tests or in local areas. Therefore these private addresses are freely usable for certain purposes. However, regulations prohibit packets having a private IP address from being transferred to a public network. An example of such a public network is the Internet. An IP address that can be used in the public networks is called a puhlic IP address. Devices nsing a private IP address have various limitations. Likewise, the devices using public IP address have various other limitations, which could be different from the ones for devices with private IP addresses.

Private and public networks are connected to one another through a gateway. Each gateway is dynamically allocated one public IP address. More public IP addresses are not allocated at least because that would increase the costs. That is, an Internet Service Provider (ISP) provides a public IP address for a gateway. This public IP address is required for connecting the gateway to the public network. Further, in a private network having a plurality of network devices, a pnblic IP address is allocated to (and used for) the gateway only. For network devices other than the gateway, arbitrary private IP addresses are internally allocated. For ensuring complete communication access with other network devices it is desirable that a device that uses a private IP address performs at least the following different tasks.

(1) It should be capable of communicating with another device inside a private network.

(2) It should be capable of connecting with a public network.

(3) A device from a public network should be able to communicate with it.

(4) It should be capable of communicating with a device in another private network.

In case (1), no obstacles exist and smooth communications are possible. In case (2), network address translation (NAT) or network address port translation (NAPT) techniques are used to translate a private IP address in a packet header to a public address as the packet is transferred from a private network to a public network. The case (3) is possible since a gateway provides a Virtual Private Network (VPN) service for connections that are requested from a public network. However, case (4) cannot be achieved with the aforementioned NAT/NAPT or VPN technology, and no conventional solutions exist.

The disclosed teachings are aimed at overcoming some of the disadvantages noted above in conventional techniques. Techniques are provided for connecting private networks dispersed in the Internet and for enabling smooth communications among devices using private IP addresses

SUMMARY

This disclosure teaches a network-connecting apparatus for a first private network having a first network device. The apparatus comprises a direct connection part for providing a direct connection in response to a connection request from the first network device, said request being a request to connect to a second network device in a second private network. Further, an address change part is provided for changing subnet numbers of origination and destination addresses of a packet transferred outside the first private network through the direct connection.

In another specific enhancement, the direct connection part comprises an address acquisition part for acquiring a public IP address of the second private network from a domain name management server based on a domain name of the second network device received from the first network device, and for acquiring a private IP address of the second network device based on the received domain name. A connection management part is provided for connecting to the second private network based on the acquired public IP address and forming a tunnel with the second private network.

More specifically, an address mapping part is provided for converting the acquired public IP address and the acquired private IP address into an address system used in the first private network in case an address system used for the public IP address of the second private network is different from the address system used for the public IP address of the first private network.

More specifically the address change part comprises a number acquisition part for receiving a unique tunnel number from the second private network, said tunnel number being allocated to the tunnel. A change part is provided for changing the subnet number of the origination address of the packet transferred outside the first private network through the direct connection to the tunnel number, and for changing the destination address of the packet to the acquired private IP address.

In another specific enhancement, a registration request part is provided for requesting a registration of a public IP address from a domain name management server, said public address being allocated from a unique domain name and internet service providing device through a communication network.

In another specific enhancement, the direct connection part includes a connection management part for forming a tunnel with the second private network having the second network device.

In another specific enhancement, the address change part comprises a number assignment part for assigning a unique tunnel number to the tunnel. A change part is provided for changing a subnet number of the origination address of the packet transferred outside the first private network through

the direct connection to the tunnel number, and for changing the destination address of the packet to a private IP address of the first network device.

More specifically, the number assignment part assigns a number that is not a subnet number of the private IP address allocated to the second network device.

In another specific enhancement, an authentication part is provided for authenticating the second network device, whereiu the direct connection part provides a direct connection in case of receiving a connection approval signal from the authentication part.

Another aspect of the disclosed teaching is a method for establishing connection between a first network device in a first private network and a second network device in a second private network. The method comprises providing a direct connection in response to a connection request from the first network device to be connected to the second network device. A private IP address of the second network device is acquired. The subnet number of an origination address of a packet transferred outside the first private network through the direct connection is changed. A destination address of the packet is changed to the private IP address of the second network device.

In another specific enhancement, the direct connection includes acquiring a public IP address of the second private network from a domain name management server based on a domain name of the second network device received from the first network device. Connection is made to the second private network based on the acquired public IP address. A tunnel is formed with the second private network.

In another specific enhancement, the direct connection further includes receiving a unique tunnel number allocated to the tunnel from the second private network. The subnet number of the origination address of the packet is changed to the tunnel number.

In another specific enhancement, prior to changing, the acquired public IP address and acquire private IP address are mapped into an address system used in the first private network address in case the address system used for the public address by the first private network is different from an address system used for the public IP address in the second private network.

In another specific enhancement, prior to direct connection, a domain name management server is requested to register a public IP address allocated from a unique domain name and internet service providing device through a communication network.

In another specific enhancement, the direct connection includes forming a tunnel with the second private network having the second network device. A unique tunnel number is allocated to the tunnel.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a structure of a network formed with network-connecting apparatuses according to an exemplary implementation of the disclosed teachings;

FIG. **2** is a block diagram of an internal structure of a network-connecting apparatus according to an exemplary implementation of the disclosed teachings;

FIG. **3** shows an IP address structure and a subnet mask according to the IPv4;

FIG. **4** shows a process of direct connections among network devices in different private networks by a network-connecting method according to an exemplary implementation of the disclosed teachings; and

FIG. **5** shows an IP packet structure passing through a tunnel formed between different private networks.

DETAILED DESCRIPTION

Hereinafter, a network-connecting apparatus and method according to exemplary implementations of the disclosed teachings will be described in detail with reference to accompanying drawings. Like reference numerals indicate like constituents respectively in drawings.

FIG. **1** shows a structure of a uetwork formed with network-connecting apparatuses according to an exemplary implementation of the disclosed teachings.

In FIG. **1** an Internet Service Provider (ISP) **110**, a Domain Name Server (DNS) **120**, a Remote Server (RS) **130**, a Remote Client (RC) **140**, and plural gateways **152**, **162**, and **172**, are connected to a public network **100**. This public network could be the Internet.

Gateway **152** acts as a passageway connecting the public network **100** and private network **150**. Likewise, **162**, and **172** act as passageways connecting private networks, **160**, and **170**, respectively, to the public network **100**. Private networks **150**, **160**, and **170** are connected to the gateways **152**, **162**, and **172** respectively. They are also connected to network devices **154***a* to **154***n*, **164***a* to **164***n*, and **174***a* to **174***n*, respectively.

The ISP **110** dynamically allocates public IP addresses in order to enable the respective gateways **152**, **162**, and **172** to connect to the Internet **100**. Dynamic allocation in this context means that the same address need not be allocated to a gateway each time a new allocation is performed for the gateway.

The domain name server **120** links an internet address to a name. The address is denoted by numbers, whereas the name is usually denoted by characters familiar to users. That is, the domain name server **120** stores and provides, to users, relations between continuously varying public IP addresses of the gateways **152**, **162**, and **172** and unique character names. Because of this, the users can easily recognize the public IP addresses of the gateways **152**, **162**, and **172** to which the users request a connection based on the names of corresponding gateways **152**, **162**, and **172**.

The RS **130** is a general remote server providing services through the Internet **100**. The RC **140** is a general client devices using a public IP address.

The gateways **152**, **162**, and **172** are network-connecting apparatuses connecting the public network **100** and the private networks **150**, **160**, and **170**. It should be noted that the gateways have both public IP addresses and private addresses. The gateways **152**, **162**, and **172** employ a public IP address while connecting to the public network **100**. On the other hand, these gateways use private IP addresses while connecting to the private networks **150**, **160**, and **170**. The respective network devices **154***a* to **154***n*, **164***a* to **164***n*, and **174***a* to **174***n* form part of the private networks **150**, **160**, and **170**, respectively. They use private IP addresses and they can be operated as servers or clients.

FIG. **2** is a block diagram showing an internal structure of a network-connecting apparatus according to an exemplary implementation of some aspects of the disclosed teachings.

In FIG. **2**, the gateway **152** has a public network interface part **205**, a private interface part **210**, a routing part **215**, a network address port translation (NAPT) part **220**, a VPN part **225**, a DNS part **230**, an IP part **235**, a direct connection part **240**, an address change part **250**, an address mapping part **260**, a user authentication part **265**, an encoding part

270, a first storage part 275, a second storage part 280, a third storage part 285, and a control part 290.

The public network interface part 205 is connected to the internet 100 through the ISP 110 and provides an interface with a broadband access network. The broadband access could be provided through Asymmetric Digital Subscriber Line (ADSL), a Cable Modem, and the like. The private network interface part 210 provides an interface with the private network 150 and employs an interface device with a LAN network having IP transfer capacity. In case the network devices 154*a* to 154*n*, that form part of the private network 150, are connected to another private network 160, the private interface part 210 modifies the address part of the packet from or to the IP part 235 with the information from the direct connection part 240. However, in other cases, the packets from or to the IP part 235 are not modified.

The IP part 235 is in charge of receiving and transferring data between the network devices 154*a* to 154*n* in the private network 150 and the network devices 154*a* to 154*n* joined in the Virtual Private Network (VPN), also the IP part 235 is in charge of receiving and transferring data between the devices 154*a* to 154*n* in the private network 150 and the RC 140 in public network. The routing part 215 performs a function of transferring data received or data to be transferred to the right destinations.

The NAPT part 220 is positioned between the public interface part 205 and the IP part 235 and translates private IP addresses into a public IP address in order to enable the plural network devices 154*a* to 154*n* that form part of the private network 150 to be connected to the Internet using only one shared public IP address. The information required for the translation are stored and updated in a NAPT translation table that is stored in the first storage part 275.

The VPN part 225 forms a tunnel in order for the RS 130 and RC 140 connected to the Internet 100 to be connected to the private network 150. Likewise the VPN part 225 also forms a tunnel in order for the network devices 164*a* to 164*n* in a second private network 160 to be connected to the private network 150. In addition, the VPN part 225 allocates private IP addresses to the RS 130, the RC 140, and the network devices 164*a* to 164*n* in the second private network 160 which are connected through the tunnel. Further, the VPN part 225 also forms a tunnel for the gateway 160 of the second private network 160 in order for the network devices 154*a* to 154*n* that form part of the private network 150 to be connected to the second private network 160.

The DNS part 230 operates as a DNS server for the private network 150. Further, on initializing the system, the DNS part 230 requests a public IP address from the ISP 110. The DNS part 230 then registers the public IP address allocated from the ISP 110 and correlates it with a unique domain name of the private network 150. The public IP address and the name are registered with the domain name server 120 connected to the internet 100.

The direct connection part 240 provides direct connections between the network devices 154*a* to 154*n* inside the private network 150 and the network devices 164*a* to 164*n* that are outside the private network 150 and form part of a second private network 160. The direct connection part 240 has an address acquisition part 242 and a connection management part 244. The address acquisition part 242 acquires a public IP address from the Domain Name Server 120. For example, 208.229.23.30, is a public IP address of the private network 160 to be connected. This could be based on a domain name of the network device 164*a*, such as "lion-.printer" that formed part of the network 160 that is waiting to be connected. This domain name is received from the network device 154*a* that forms part of the private network 150. The connection management part 244 is connected to a gateway of the private network 160 (that is waiting to be connected), on a basis of the acquired IP address, to form a tunnel.

If the tunnel with the to-be-connected private network 160 is formed, the address acquisition part 242 transfers the domain name of the network device 164*a* (the device whose connection is desired) to the gateway of the to be-connected private network 160. The address acquisition part 242 receives a private IP address of the corresponding network device 164*a* from the corresponding gateway 162. The address acquisition part 242 changes a subnet number of the private IP address of the corresponding network device 164*a* to a tunnel number. The address acquisition part 242 then transfers the tunnel number to the network device 154*a* requesting the connection.

The connection-requesting network device 154*a* grasps that IP packets to be sent to the to-be-connected network device 164*a* and then transfer them to the gateway 162 of the private network 160 to which the network device 164*a* belongs. The transfer is done using the process of Address Resolution Protocol (ARP) and is based on the changed private IP address of the to-be-connected network device 164*a* that is transferred to 154*a*. In order for two hosts to communicate in a virtual network, physical network addresses should be obtained from the respective hosts and then matched with IP addresses. The ARP is a protocol that performs a broadcast function in a network such as the Ethernet.

The private IP address of the to-be-connected network device 164*a* received from the gateway 162 of the private network to be connected is recorded in a translation table stored in the second storage part 275. Likewise, the private IP address of the connection-requesting network device 154*a*, and the tunnel number are also recorded in the translation table stored in the second storage part 275.

The connection-requesting network device 154*a* produces an IP packet designating a destination address. This designating address is formed by changing a subnet number of the private IP address of the to-be-connected network device 164*a* changed in a subnet number. It then makes a transfer request. The address change part 250 changes a subnet number of an originating address of the produced IP packet to a tunnel number. It also changes the destination address of the produced IP packet to a private IP address of the to-be-connected network device 154*a*. In the meantime, the address change part 250 reads out the private IP address of the to-be-connected network device 164*a*, the private IP address of the connection-requesting network device 154*a*, and the tunnel number from the translation table stored in the second storage part 280 and performs an address change process.

The address change part 250 has a number acquisition part 252, a number assignment part 254, and a change part 256. The number acquisition part 252 receives a unique tunnel number which is assigned to a tunnel formed from the gateway 162 of the to-be-connected private network 160. The number assignment part 254 provided in the gateway 162 of the to-be-connected private network 160 assigns the tunnel number. When the gateway 162 of the to-be-connected private network 160 assigns a tunnel number, the gateway 162 considers a sub-netting method of the private network 160 corresponding to the gateway 162. That is, subnet numbers not assigned to the network devices 164*a* to 164*n* existing in the private network 160 corresponding to the gateway 162 are assigned as tunnel numbers. It is

preferable that the number acquisition part **252** and the number assignment part **254** must cooperate to make the unique tunnel number. The change part **256** changes the origination and destination addresses of an IP packet.

If two gateways **152** and **162** use the same sub-netting method, all subnet numbers not assigned from both private networks **150** and **160** only may be assigned as tunnel numbers. In the meantime, when the gateway **162** of the to-be-connected private network **160** assigns tunnel numbers, the gateway **162** may exchange sub-netting information with a connection-requesting gateway **152**. This exchange of information is done such that the subnet numbers not used in both the gateways **152** and **162** can be used as tunnel numbers. In either case, it is desirable that the subnet numbers of private IP addresses used in the respective private networks **150** and **160** are fixed. This is done such that the subnet numbers not allocated in the respective private networks **150** and **160** can be allocated as tunnel numbers.

Information on the origination and destination addresses is generally included in an IP packet header. However, some network codes require that information about an address is included in a payload portion of an IP packet. Therefore, it is desirable that the gateway **152** has a packet identification part (not shown). This packet identification part can extract IP address information from an IP packet transferred from a private network in accordance with such network codes.

An IP packet in which an address change is completed is transferred to the gateway **162** of the to-be-connected private network **160** through a tunnel formed between the respective private networks **150** and **160**. The gateway **162** of the to-be-connected private network **160** transfers a received IP packet to the to-be-connected network device **164***a*.

In some instances an IP address system used in the private network **150** to which the connection-requesting network device **154***a* belongs is different from an IP address system used in the private network **160** to which the to-be-connected network device **164***a* belongs, for example IPv4. In such a case, the address mapping part **260** converts the address into a particular IP address system such as IPv6. The conversion of an IP address system employs a method using a router and a domain name server which support both IPv4 and IPv6. It also employs a method for encapsulating an IPv6 diagram in an IPv4 packet, and so on. Detailed descriptions of these methods are omitted since they are well known to one skilled in the art.

A user authentication part **265** carries out an authentication process when connection requests originate from network devices **164***a* to **164***n*, RS **130**, and RC **140**, that do not form part of the private network **150**. User information necessary for user authentications is stored in the third storage part **285**. Preferably, the direct connection part **240** forms a tunnel and provides a direct connection in case of receiving a connection approval signal for a network device such as the network device **164***a* requesting a connection from the user authentication part **265**.

The encoding part **270** encodes data in case such additional security is required for packets communicating with devices connected to the Internet **100**. Further, the encoding part **270** decodes the data received through the Internet **100**. Information necessary to carry out the encoding and decoding of packets in the encoding part **270** is stored in the third storage part **285**. The control part **290** controls the operations of the respective constituents of the overall system.

FIG. **3** shows an IP address structure and a subnet mask according to the IPv4 protocol.

In FIG. **3**, an IP address is structured with a network address part **310** and a host address part **320**. A network is normally separated internally into several segments for better management. At this time, the host address part **320** of the IP address **300** is divided into a subnet number part **330** and a host number part **340**. The subnet mask **350** is used to designate a broadcasting range. Basically, the communication method of the Local Area Network (LAN) is the broadcasting method, separating one network class into plural network segments using subnet masking. This enables IP addresses to be efficiently used. FIG. **3** shows a subnet mask **350** set to 255.255.255.0. Therefore, the subnet number part **330** of a 32-bit IP address **300** is included in a network number.

FIG. **4** shows a process of direct connections among network devices existing in different private networks by a network-connecting method according to an exemplary implementation of some aspects of the disclosed teachings.

In FIG. **4**, a TV **405** that is part of a network A **410** having a domain name of tiger.tv requests a direct connection to a printer **465** existing in a network B **460** and having a domain name of lion.printer (S**400**). Both the TV **405** and the printer **465** have network functions. The TV **405** transfers the domain name of the printer **465** to a gateway A and makes the request. The gateway A **420** transfers the domain name of the printer **465** to a domain name server **440** holding public IP addresses of the network A **410** and network B **460**. It then requests a public IP address of a private network to which the printer **465** belongs (S**405**). The domain name server **440** provides the public IP address of the network B corresponding to the domain name of the printer **465** transferred from the gateway A **420** to the gateway A **420** (S**410**).

The gateway A **420** connects to the gateway B **450** and requests a tunnel formation (S**415**).

The gateway B **450** creates a tunnel having a unique tunnel number TN (S**420**). Prior to creating the tunnel, the gateway B **450** carries out a user authentication process and checks if TV **405** requesting the connection has the necessary connection authority. The tunnel is created only if such an authorization exists.

The gateway B **450** allocates the subnet numbers not assigned to network devices, existing in the network B **460**, as tunnel numbers. If the respective networks **410** and **460** use the same sub-netting method, the subnet numbers not allocated in all of the respective networks **410** and **460** may be allocated as tunnel numbers.

When the gateway B **450** allocates a tunnel number, the gateway B **450** exchanges sub-netting information with the gateway A **420** and then allocates as a tunnel number a subnet number not used in all of the respective networks **410** and **460**. In either case, the subnet number parts of private IP addresses used in the respective networks **410** and **460** are preferably fixed so that a subnet number not assigned in the respective networks **410** and **460** can be allocated as a tunnel number.

Once a tunnel is formed, the gateway A **420** requests a private IP address of the printer **465** to the gateway B **460** (S**425**). The gateway B **460**, in response to the request, provides a private IP address 172.16.0.9 of the printer **465** to the gateway B **420** (S**430**). The gateway A **420** converts the provided subnet number of the private IP address of the printer **465** to a tunnel number and then transfers the tunnel number to the TV **405** (S**435**).

The TV **405** requests a transfer of IP packets in which its own private IP address and the converted private IP address of the printer **465** transferred from the gateway A **420** are recorded as the origination and destination addresses respec-

tively (S440). The origination and destination addresses of the IP packet transferred to the gateway A **420** from the TV **405** are 172.16.0.6 and 172.16.TN.9 respectively. In this case, TN is the allocated tunnel number. The gateway A **420** converts a subnet number of the origination address of the IP packet received from the TV **405** to a tunnel number, changes the destination address to a private IP address of the printer **465**, and transfers the IP packet to the gateway B **450** (S445). Through such a conversion process, the origination and destination addresses of the IP packet transferred to the gateway B **450** from the gateway A **420** are converted into 172.16.TN.6 and 172.16.0.9 respectively.

The gateway B **460** transfers the received IP packet to the printer **465** (S450). After carrying out the step S450, in case that there is a transfer request of the IP packet from the printer **465** to the TV **405** or from the TV **405** to the printer **465**, the respective gateways **420** and **460** carries out the steps S440 to S450 to provide direct communications between the TV **405** and the printer **465** (S455 to S465).

FIG. **5** shows an IP packet passing through a tunnel formed between the gateway A **420** and the gateway B **460**. The respective gateway **420** and **460** processes the exchange of an IP packet header tunnel number and a subnet number in the packet header of the TV/printer in a private network.

In the above exemplary implementation of the disclosed teachings, the description has been made on packet exchanges through a direct connection among network devices existing in a network having an address system according to the IPv4. However, one skilled in the art may understand that the network-connecting apparatus and method may be applied to a direct connection among network devices existing in a network having an address system according to the IPv6 and to a direct connection among network devices existing in a network having different address systems.

With the network-connecting apparatus and method according to the disclosed teachings, a direct connection between network devices existing in different private networks is possible. Therefore, it is available to provide new services such as P2P services, Home-to-Home services, and the like, using a private network. In addition, even in information exchanges, secrecy may be guaranteed since information is not recorded in a storage device of an internet service provider, as well as perfect security may be maintained with application of individual security codes between private networks.

Although the preferred embodiment of the present invention has been described, it will be understood by those skilled in the art that the present invention should not be limited to the described preferred embodiment, but various changes and modifications can be made within the spirit and scope of the present invention as defined by the appended claims.

What is claimed is:

1. A network-connecting apparatus for a first private network having a first network device, the apparatus comprising:

a direct connection part for providing a direct connection by forming a tunnel with a second private network in response to a connection request from the first network device, said request being a request to connect to a second network device in a second private network, wherein the direct connection part comprises:

an address acquisition part for acquiring a public IP address of the second private network from a domain name management server based on a domain name of the second network device received from the first network device, and for acquiring a private IP address of the second network device based on the received domain name, wherein the acquired private IP address is a destination address having a subnet number of the destination address of a packet to be transferred outside the first private network; and

a connection management part for connecting to the second private network based on the acquired public IP address and forming the tunnel with the second private network:

an address mapping part for converting the acquired public IP address and the acquired private IP address into an address system used in the first private network in case an address system used for the public IP address of the second private network is different from the address system used for the public IP address of the first private network; and

an address change part for changing the subnet number of the destination address through the direct connection to a tunnel number allocated to the tunnel, changing a subnet number of an origination address of the packet to the tunnel number, and changing the tunnel number of the destination address to the subnet number of the destination address when the packet is transferred to the second network device.

2. The network-connecting apparatus as claimed in claim **1**, wherein the address change part comprises:

a number acquisition part for receiving the tunnel number from the second private network; and

a change part for changing the subnet number of the origination address of the packet transferred outside the first private network through the direct connection to the tunnel number, and for changing the destination address of the packet to the acquired private IP address.

3. The network-connecting apparatus as claimed in claim **1**, further comprising:

a registration request part for requesting a registration of a public IP address from the domain name management server, said public address being allocated from a unique domain name and internet service providing device through a communication network.

4. The network-connecting apparatus as claimed in claim **1**, wherein the address change part comprises:

a number assignment part for assigning the tunnel number to the tunnel; and a change part for changing the subnet number of the origination address of the packet transferred outside the first private network through the direct connection to the tunnel number, and for changing the destination address of the packet to the private IP address of the second network device, wherein the private IP address is the destination address having the subnet number of the destination address.

5. The network-connecting apparatus as claimed in claim **4**, wherein the number assignment part assigns a number that is not a subnet number of the private IP address allocated to be the second network device.

6. The network-connecting apparatus as claimed in claim **1**, further comprising an authentication part for authenticating the second network device, wherein the direct connection part provides a direct connection in case of receiving a connection approval signal from the authentication part.

7. A network-connecting method for establishing connection between a first network device in a first private network and a second network device in a second private network, the method comprising:

a) providing a direct connection in response to a connection request from the first network device to be con-

nected to the second network device, wherein the providing of the direct connection comprises;

ai) acquiring a public IP address of the second private network from a domain name management server based on a domain name of the second network device received from the first network device;

aii) connecting to the second private network based on the acquired public IP address; and

aiii) forming a tunnel with the second private network;

b) forming the tunnel to which a unique tunnel number is allocated;

c) acquiring a private IP address of the second network device;

d) changing a subnet number of the acquired private IP address of the second network device to the tunnel number;

e) changing a subnet number of an origination address of a packet transferred outside the first private network through the direct connection to the tunnel number; and

f) changing the tunnel number of the acquired private IP address of the second network device to the subnet number of the acquired private IP address of the second network device when the packet is transferred to the second network device.

wherein prior to operation d), the acquired public IP address and acquired private IP address are mapped into an address system used in the first private network address in case the address system used for the public address by the first private network is different from an address system used for the public IP address in the second private network.

8. The network-connecting method as claimed in claim **7**, wherein prior to the direct connection, the domain name management server is requested to register a puhlic IP address allocated from a unique domain name and internet service providing device through a communication network.

* * * * *

EXHIBIT 1007

U.S. Patent Application Publication No. 2003/0028671 to *Mehta et al.* ("*Mehta*")

US 20030028671A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0028671 A1**

Mehta et al. (43) **Pub. Date: Feb. 6, 2003**

(54) **METHOD AND SYSTEM FOR TWO-WAY INITIATED DATA COMMUNICATION WITH WIRELESS DEVICES**

(75) Inventors: **Samir Narendra Mehta**, Renton, WA (US); **Mazin Ramadan**, Seattle, WA (US); **Geoffrey S. Heller**, Seattle, WA (US); **Vineet R. Sharma**, Renton, WA (US); **Markus L. Jansen**, Renton, WA (US); **Edward L. Gow**, Seattle, WA (US); **Ngochan T. Nguyen**, Seattle, WA (US)

Correspondence Address:
SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVE
SUITE 6300
SEATTLE, WA 98104-7092 (US)

(73) Assignee: **4th pass Inc.**, Seattle, WA

(21) Appl. No.: **10/167,240**

(22) Filed: **Jun. 10, 2002**

Related U.S. Application Data

(60) Provisional application No. 60/296,902, filed on Jun. 8, 2001.

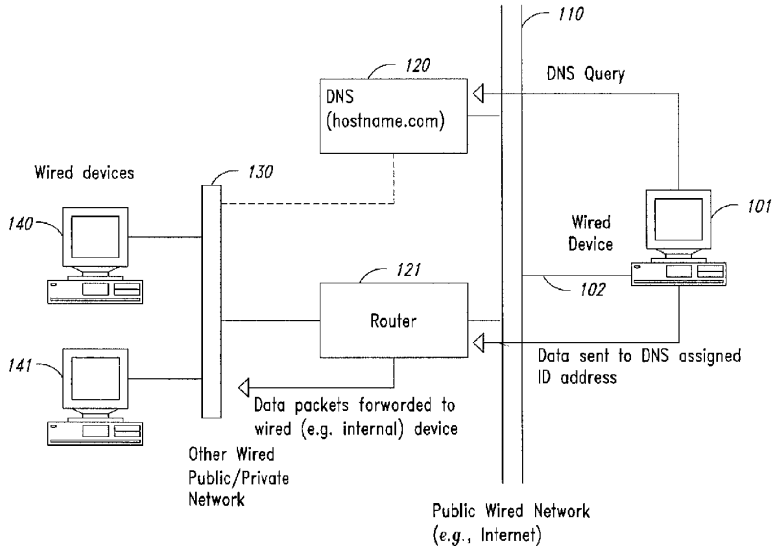
Publication Classification

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/245**; 709/230

(57) **ABSTRACT**

Methods and systems for providing two-way initiated, bi-directional communication with wireless devices using connection-based or connection-less protocols, such as, for example, TCP/IP and UDP/IP, are provided. Example embodiments provide an Address Management Proxy System ("AMPS"), which enables devices and systems connected to a public internet, such as the Internet, to initiate communication with and to send data to wireless devices connected to a private wireless network, without exposing the non-routable private addresses of these wireless devices. The AMPS allocates a public (routable) network address for temporarily use by a requesting device on a public network to communicate with a wireless device on a wireless network. In one embodiment, a pool of public addresses, for example, public IP addresses, is maintained by the AMPS and allocated dynamically to wireless network devices as required. In one embodiment, the AMPS comprises one or more modified DNS/API servers, one or more Address Proxy/Routers, an Address Management Data Server, one or more data repositories, and optionally a load balancer. The AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device, and returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device. The public address is then usable by the device on the public network to send data to the wireless device.



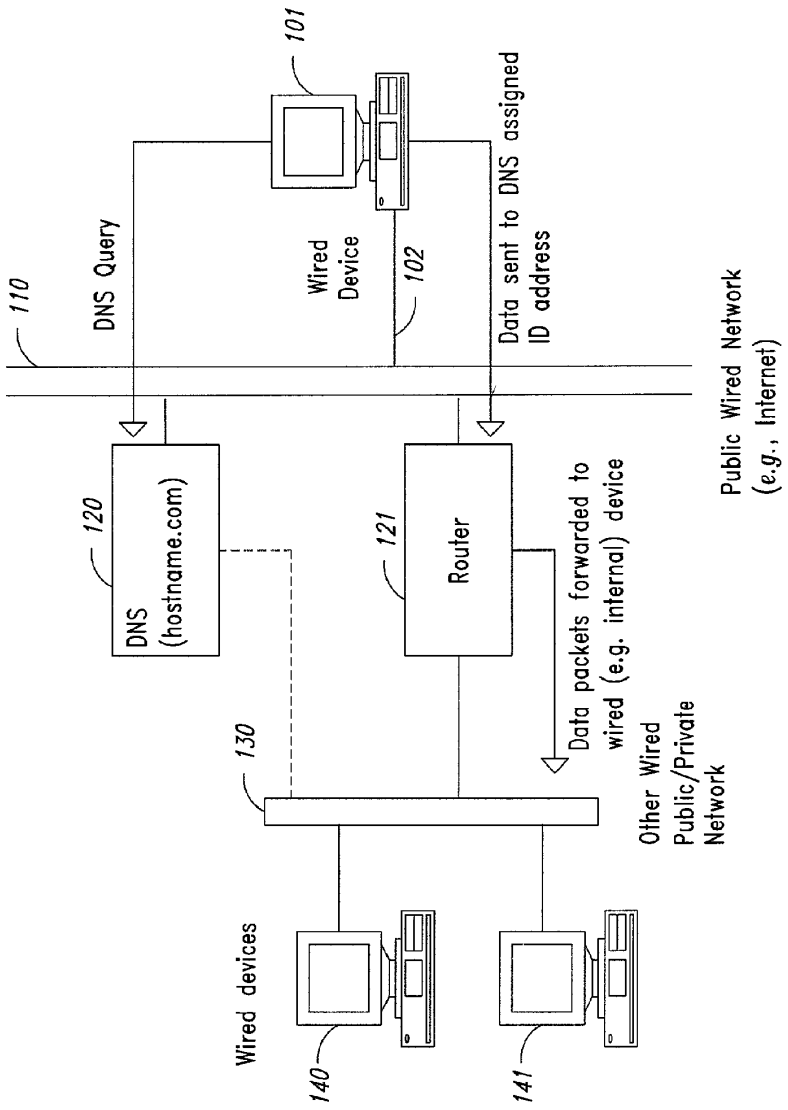


Fig. 1

AA/SWA Ex. 1015, p.62 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

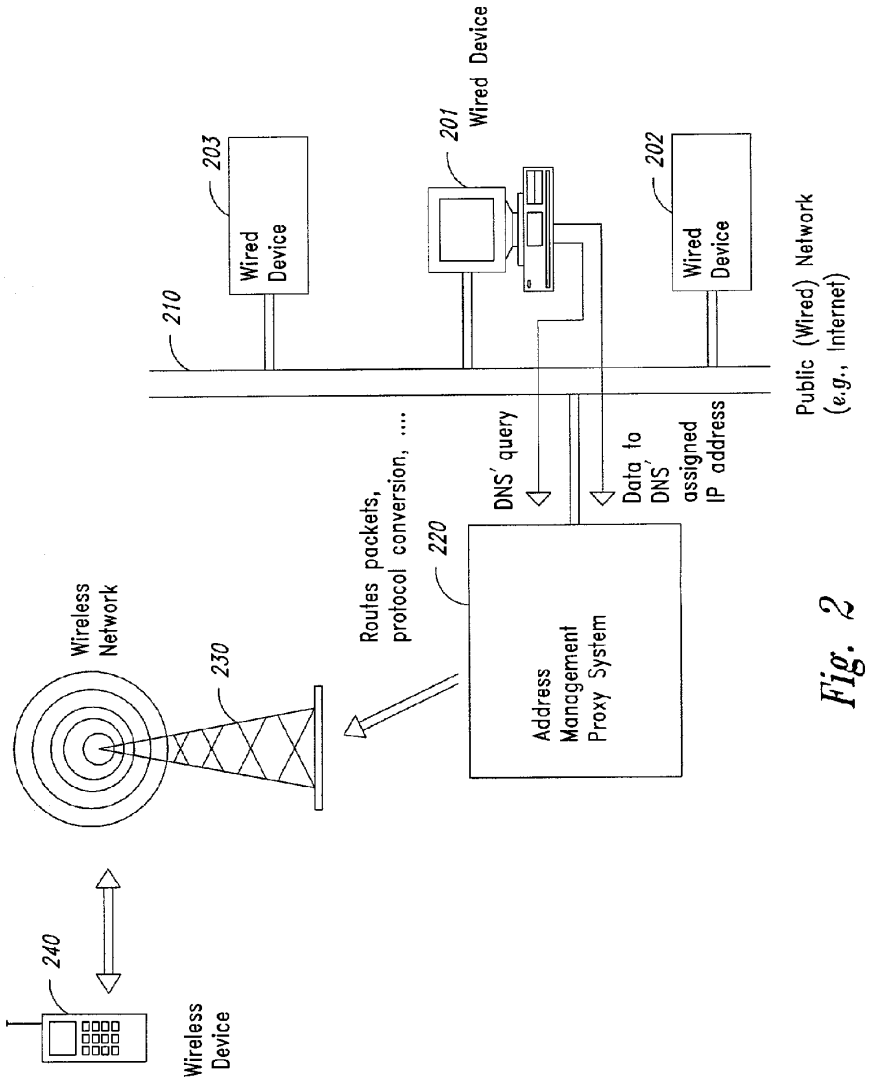


Fig. 2

AA/SWA Ex. 1015, p.63 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

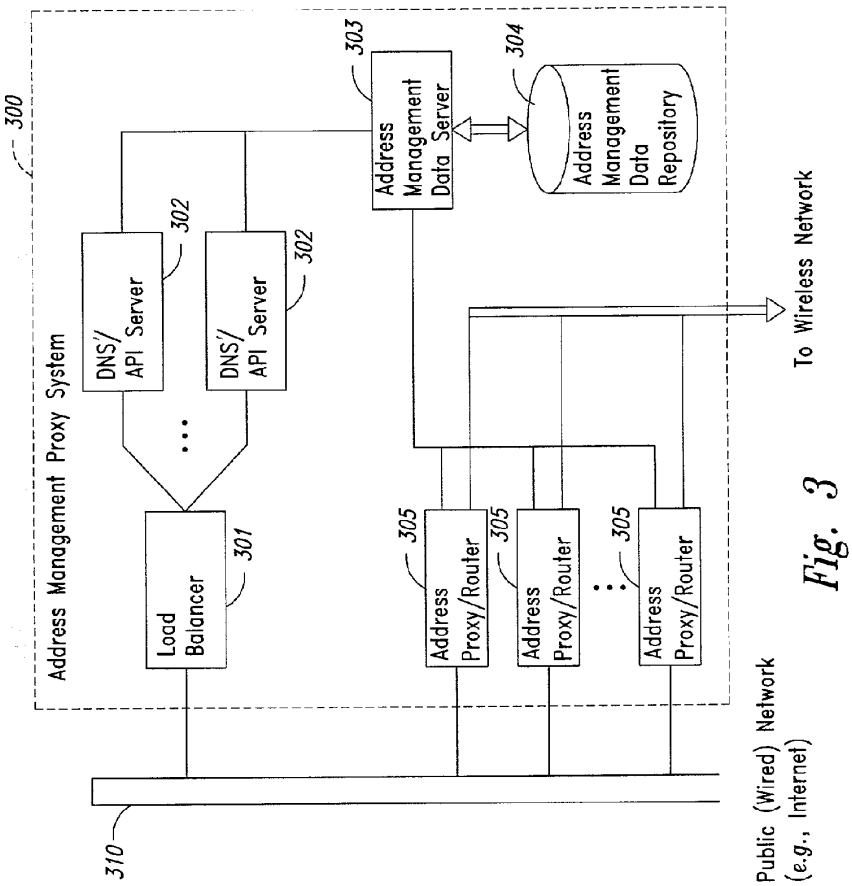

300
Address Management Proxy System
303
Address Management Data Server
304
Address Management Data Repository
302
DNS/ API Server
302
DNS/ API Server
301
Load Balancer
305
Address Proxy/Router
305
Address Proxy/Router
305
Address Proxy/Router
To Wireless Network
310
Public (Wired) Network (e.g., Internet)

Fig. 3

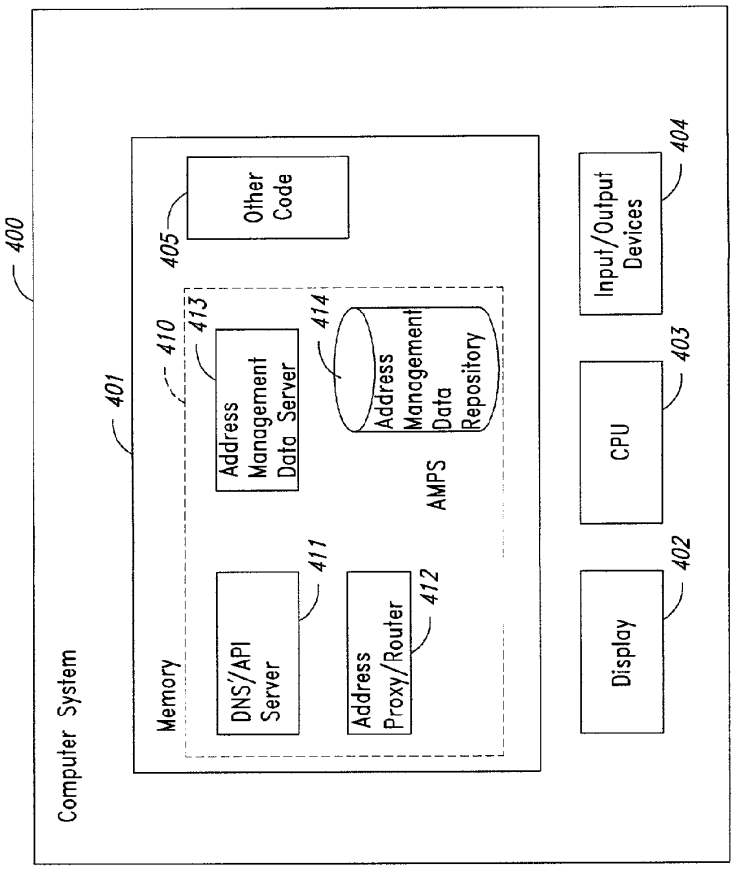

400
Computer System
401
Memory
410
413
Address Management Data Server
414
Address Management Data Repository
AMPS
405
Other Code
411
DNS/API Server
412
Address Proxy/Router
402
Display
403
CPU
404
Input/Output Devices

Fig. 4

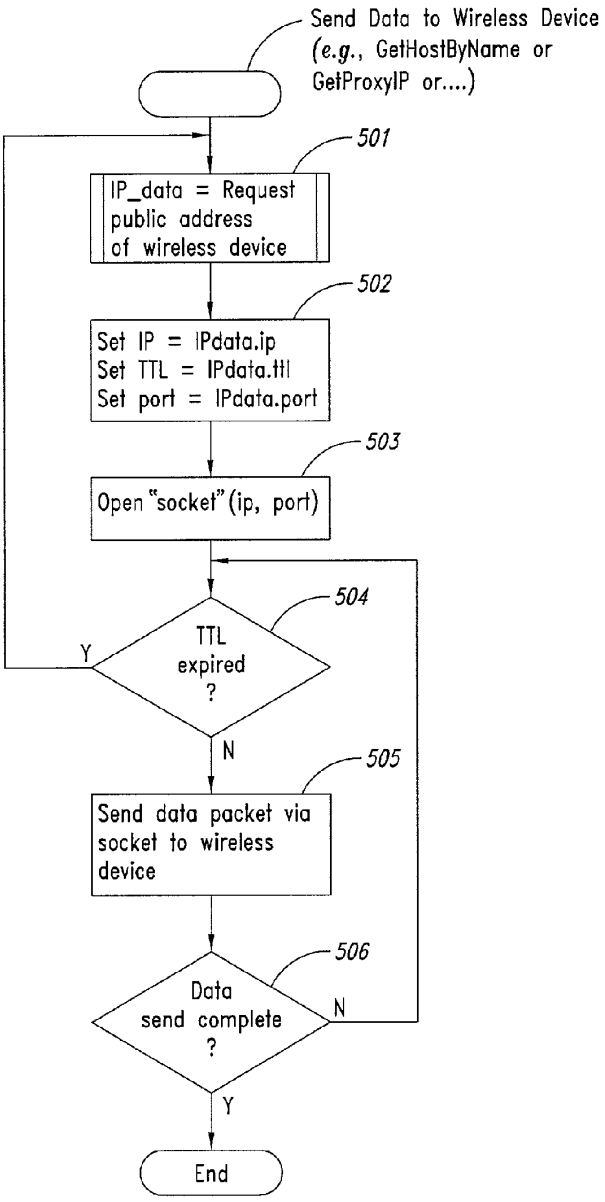

Send Data to Wireless Device
(e.g., GetHostByName or
GetProxyIP or....)
501
IP_data = Request
public address
of wireless device
502
Set IP = IPdata.ip
Set TTL = IPdata.ttl
Set port = IPdata.port
503
Open "socket" (ip, port)
504
TTL
expired
?
Y
N
505
Send data packet via
socket to wireless
device
506
Data
send complete
?
N
Y
End

Fig. 5

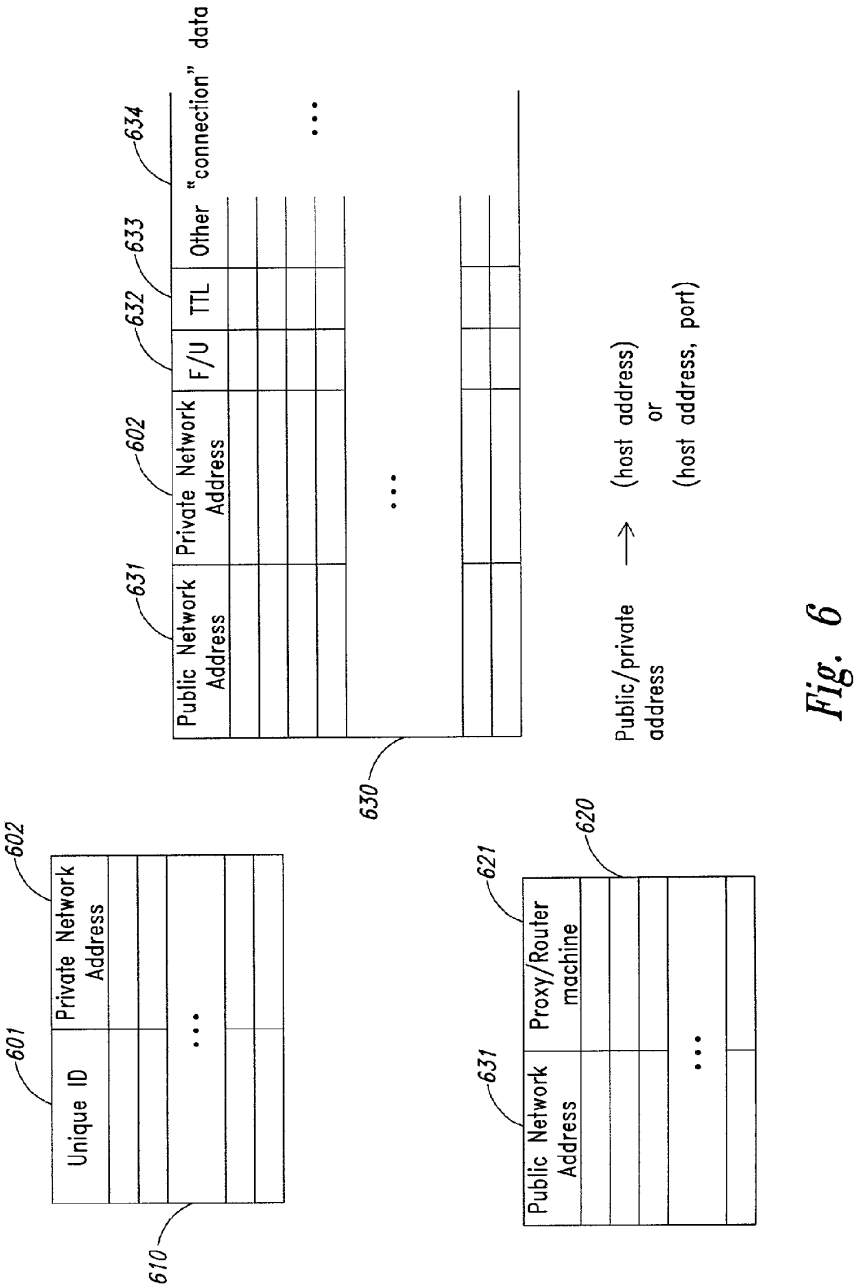


Fig. 6

AA/SWA Ex. 1015, p.67 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

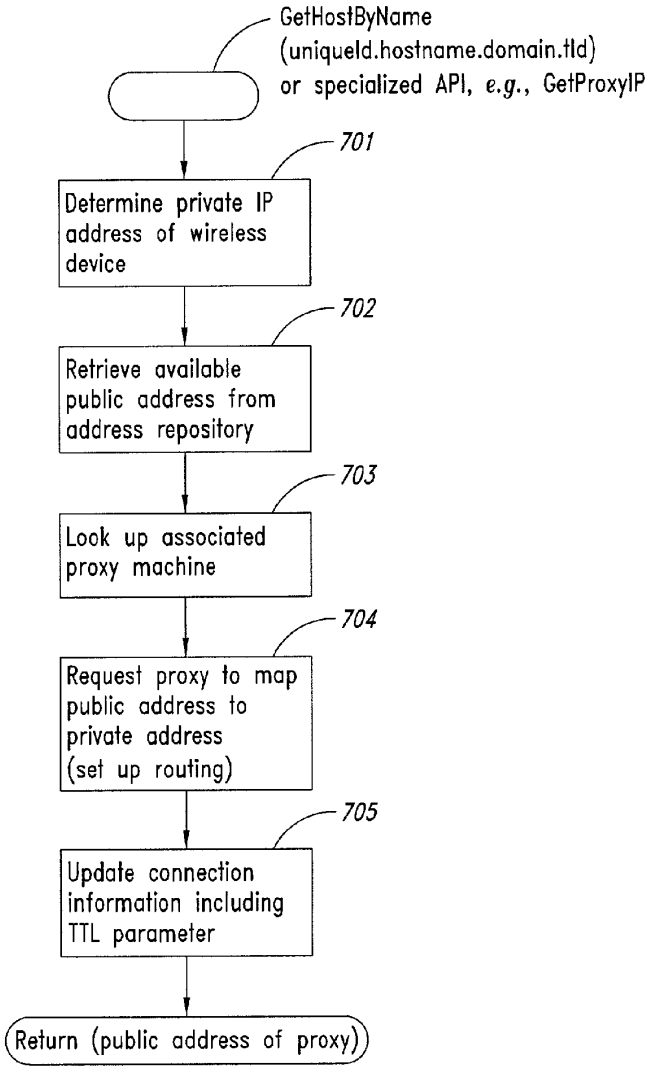

GetHostByName
(uniqueId.hostname.domain.tld)
or specialized API, e.g., GetProxyIP
701
Determine private IP address of wireless device
702
Retrieve available public address from address repository
703
Look up associated proxy machine
704
Request proxy to map public address to private address (set up routing)
705
Update connection information including TTL parameter
Return (public address of proxy)

Fig. 7

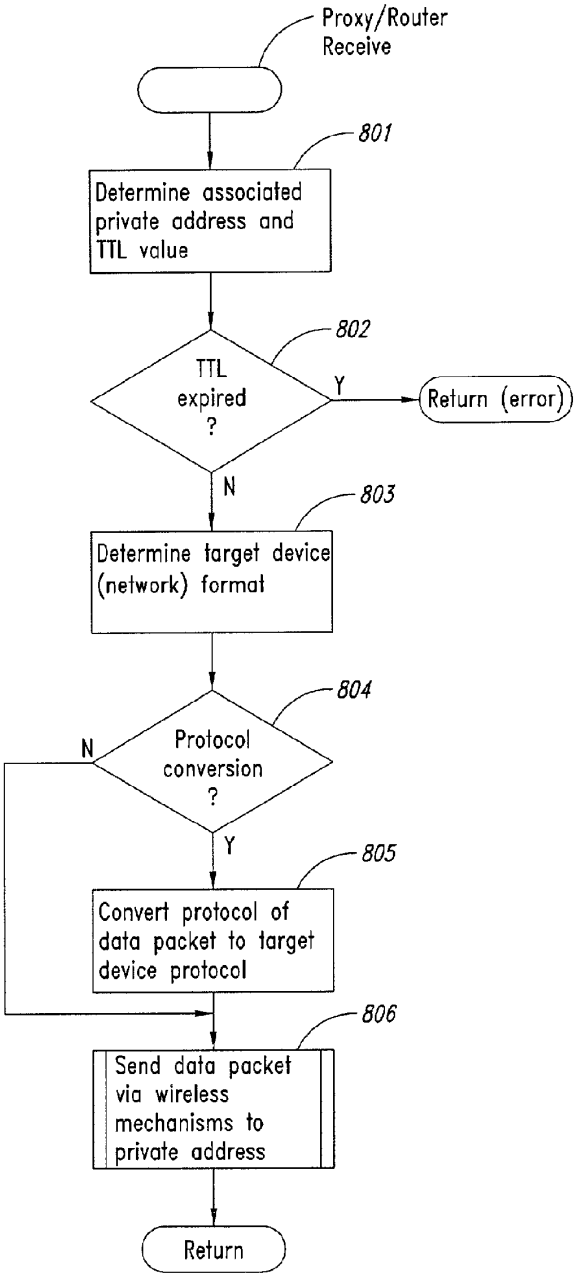

Proxy/Router Receive
801
Determine associated private address and TTL value
802
TTL expired ?
Y
Return (error)
N
803
Determine target device (network) format
804
Protocol conversion ?
N
Y
805
Convert protocol of data packet to target device protocol
806
Send data packet via wireless mechanisms to private address
Return

Fig. 8

METHOD AND SYSTEM FOR TWO-WAY INITIATED DATA COMMUNICATION WITH WIRELESS DEVICES

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to methods and systems for initiating communication with wireless devices and, in particular, to methods and systems for initiating communication with a device on a private network from a device on a public network to achieve virtual end-to-end connectivity.

[0003] 2. Background Information

[0004] The need to connect networked computers together with other networks of computers has become increasingly important as our global society strives to communicate for business and personal reasons on an international level. This need has driven the technical community to devise ways to interconnect devices on different physical networks so that devices on heterogeneous and homogeneous networks can communicate with one another as in a uniform (or standard) manner. Such interconnection technology is often referred to as "internetworking,""internetworks," or simply "internets." One such global internetworking implementation is the Internet (first letter capitalized to distinguish from "internets" generally), as originally developed by the ARPA, NSF, etc. for educational and government purposes. The Internet, in its now expanded version, exists as a complex infrastructure of network backbones that connect to networks around the world. Other (local, regional, private, or public) networks connect to the Internet backbone by means of gateways or routers (also known as gateway servers, gateway systems, router servers, and router systems). For purposes of this document, the term "router" or "gateway," used alone or to modify another noun, are used interchangeably and will refer generically to any hardware or software, subsystem, system, or code that is able to transfer a data packet (at any level of the network or physical data transfer) between two or more homogeneous or heterogeneous machines, systems, or subsystems, without regard to a particular gateway/router machine or service. In the Internet environment, the presence of a router or gateway typically indicates an ability to route an Internet datagram to another router or machine. Machines intended to run applications are generally referred to using networking terminology as "hosts" or "host machines;" for purposes herein, a router/gateway may be a function of a host machine or may be a separate device.

[0005] In the Internet environment, the various networks and devices communicate using standard network protocols and models, such as TCP/IP (or UDP/IP). Although for the purpose of this document, the reader is presumed to be familiar with networking concepts, protocols, and standards, a brief summary is provided herein for ease. Extensive background information of internetworking, internets, the Internet, and related terms and background technology can found in Tanenbaum, A., *Computer Networks,* Prentice-Hall, N.J., 3d ed. 1996, and in Comer, D., *Internetworking with TCP/IP, Principles, Protocols, and Architectures,* Prentice Hall, N.J., 4th ed. 2000, which are herein incorporated by reference in their entirety.

[0006] TCP/IP and UDP/IP (or often referred to as "UDP") refer to a popular transport layer and network layer protocol combinations, which are commonly found in internetworking environments (other protocols are available at each of these layers as well). The "IP" in TCP/IP, refers to "Internet Protocol," and is a network layer protocol that defines how data is organized and represented (the format and meaning of datagrams) and the communications transactions used to route them. TCP ("Transmission Control Protocol") and UDP ("User Datagram Protocol"), which are both transport layer protocols that can be implemented on top of an IP protocol, support connection-based and connectionless data transfer, respectively. Connection-based data transfer implies that a source and destination device request a connection and then send data to each other over the "virtual" connection in a manner that is sequenced (and typically involves handshaking mechanisms). The term "virtual" here implies that, although the connection is not necessarily hard-wired, the connection appears to provide a direct conduit between a source (requestor) and destination (receiver). The data actually flows through lower protocol layers to be eventually transmitted over a physical transmission medium. Connection-less data transfer implies that the source sends a datagram to the destination, but doesn't insure delivery or that data will arrive in a particular order.

[0007] The IP protocol also defines a uniform network addressing mechanism, so that machines that implement protocols that use IP, such as TCP or UDP, are able to specify sources and destinations for their data transfers. The network addressing mechanism specifies an abstract address and a binding protocol for mapping the abstract address to a physical hardware address. For purposes of this description, the uniform network addressing mechanism will be referred to generically as an "IP address." IP addresses are often written in "dotted decimal" notation, which specifies an address as "w.x.y.z" (e.g., in a 32-bit address, each letter designates a byte of information). For example, an IP address such as "192.251.0.1" may specify a host machine at network "192," subnet "251," and domain "0." Using IP, typically a range of addresses are reserved for private network use and the remaining IP addresses are either reserved for other uses or for public (routable) addresses, which are assigned by an authority organization. Multiple private networks may assign the same (non-routable) IP addresses internally (currently the Internet Corporation for Assigned Names and Numbers, ICANN), but use unique public IP addresses to connect to the Internet. For example, in Class B networks (which, using class-based addressing conventions, allow up to 254 host machines each), private addresses may range from 192.168.0.0 to 192.168.255.0. Addressing conventions are well known to one skilled in the art and are presumed known to the reader. For purposes of this application, an IP address is understood to be whatever address makes sense (and is defined) in a particular internetworking environment, although examples which use Internet IP addressing may be referred to.

[0008] A network that supports IP can be connected to another TCP/IP-based or UDP/IP-based internet or the Internet, by providing a router which forwards data to another router or host machine based upon an IP address. The router (or routing server/service) typically contains a routing table, which determines to which machine (and optionally to which port) to send a datagram, given a destination IP address. The IP address uniquely identifies a router/host machine, and, in a typical TCP/IP network, can be mapped to a string name that identifies, for example, a particular

AA/SWA Ex. 1015, p.70 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

machine as part of a larger domain. (Although referred to herein often as a TCP/IP-based network, one skilled in the art will recognize that the network may also be UDP-based (connectionless), and may support another session management system.)

[0009] In a typical TCP/IP (inter)network, machines are organized according to a naming hierarchy. One such hierarchy is the Domain Name System ("DNS"), which specifies how a particular machine is connected to others. (The term DNS is sometimes used also to identify a server or service that implements the DNS protocol.) For example, the string "initials_machine.4thpass.service_provider.com," may be used to specify a machine belonging to you and connected to the 4thpass company LAN, which is in turn connected to a service_provider's WAN (wide area network). TCP/IP and UDP/IP define tools/libraries for client systems to use to determine an IP address (a logical address on an internet) given a string name of a particular router/machine. One such tool is referred to as a DNS query and includes, for example, an API called "GetHostByName." GetHostByName returns an IP address given a string. A server machine that implement the DNS standard for a particular organization, network, or subnetwork is referred to herein simply as a DNS, although DNS services may be provided in conjunction with other networking services on a single physical machine.

[0010] **FIG. 1** is an example block diagram of basic Internet or internet communication to send a data packet using TCP/IP or UDP/IP. In **FIG. 1**, a host machine **101** is shown connected to the Internet **110** via wire **102**. Other wired devices, such as host machines **140** and **141**, are shown connected to a private (or public) network **130**, which could be, for example, a local area network (LAN). The devices on network **130** communicate over the Internet **110** by means of an additional machine, a router **121**, which is shown connected via a wire (e.g., a phone line). A DNS server **120** is shown, also connected via a wire, to Internet **110**. In basic typical operation source device (host machine) **101**, intending to send a data packet to device **140** (via TCP or UDP), first performs a DNS query to obtain an IP address that corresponds to a string name that represents the device **140**. For example, to send data to "initials_machine.4thpass.service_provider.com," DNS **120**, may correspond to a DNS server for "4thpass.com." This server knows how to locate machines in its "domain," for example, the "initials_machine", and can retrieve their corresponding public IP addresses. Upon determining the correct (public) IP address, the DNS **120** returns this address to the source device **101**. The source device **101** then can either open up a TCP connection to communicate with the destination device **140** or simply send packets via UDP or other connection-less protocol using the returned public IP address.

BRIEF SUMMARY OF THE INVENTION

[0011] Embodiments of the present invention provide computer- and network-based methods and systems for two-way initiated, bi-directional communication with wireless devices using connection-based or connection-less protocols, such as, for example, TCP/IP and UDP/IP. Example embodiments provide an Address Management Proxy System ("AMPS"), which enables devices and systems connected to a public internetwork, such as the Internet, to initiate communication with and send data to wireless devices connected to a private wireless network, without exposing the non-routable private addresses of these wireless devices. The AMPS allocates a public (routable) network address for temporary use by a requesting device on an external public network to communicate with a wireless device on a private wireless network. In one embodiment, a pool of public addresses, for example, public IP addresses, is maintained by the AMPS and allocated dynamically to wireless network devices as required. The mapping of a temporary public address to the private address of a wireless device is maintained and updated transparently by the AMPS using routing tables and other mapping data structures.

[0012] In one embodiment, the AMPS comprises one or more modified DNS/API servers, one or more Address Proxy/Routers, an Address Management Data Server, one or more Address Management Data Repositories, and optionally a load balancer. The AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device, and returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device. The public address is then usable by the device on the external public network to send data to the wireless device. The temporary public address is, for example, an address associated with one of the Address Proxy/Routers, which are connected to the external public network and have access to the private addresses on the private wireless network. In some cases, the device on the public network that desires to send data to the wireless device uses a connection-based protocol, such as TCP/IP to send data. In other cases the device uses a connection-less protocol, such as UDP (UDP/IP) to send the data.

[0013] According to one approach, the AMPS provides a modified DNS server that changes what is returned as a result of a call to a standard DNS query function, such as GetHostByName. In another approach, the AMPS implements a specialized API for a device on a public network to use to query for a public address of a designated wireless device. Using a specialized API implementation in conjunction with Internet Protocol, the AMPS can map private address to addresses that comprise only IP addresses, or can map to an (IP address, port) pair. This latter implementation can extend the usefulness of a particular public address space.

[0014] The AMPS techniques can be used by a wired device on a private or public network and by a wireless device on such a network acting in a capacity of a source device, as long as the device is connected to a public network that can address and be addressed by the AMPS. Thus, the AMPS mechanisms can be used by devices on different private wireless networks to communicate with one another. In addition, the AMPS mechanisms can be used with other internetworks, such as ATM networks and with data transfer protocols other than TCIP/IP or UDP.

[0015] To insure a greater degree of security, according to one embodiment, the AMPS maintains a Time to Live (TTL) parameter with each address mapping. In this way, once the TTL value indicates that the mapping has expired, the AMPS can destroy the mapping, and also any connection. Further, in some embodiments, the AMPS also puts a timestamp in its own mapping tables. After some timeout

period based upon the timestamp, the AMPS can destroy the mapping, thereby forcing a new mapping to be initiated on a periodic basis.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] **FIG. 1** is an example block diagram of basic Internet or internet communication to send a data packet using TCP/IP or UDP/IP.

[0017] **FIG. 2** is a block diagram of an example Address Management Proxy System used in bi-directional communication with a wireless device.

[0018] **FIG. 3** is an example block diagram of components of an example Address Management Proxy System.

[0019] **FIG. 4** is an example block diagram of a general purpose computer system for practicing embodiments of the Address Management Proxy System.

[0020] **FIG. 5** is an example flow diagram of the process performed by a device on a public network to send data to a wireless device located on a private wireless network using the Address Management Proxy System.

[0021] **FIG. 6** is an example block diagram of some of the Address Management Proxy System data repository tables used to support routines of the DNS'/API servers and the Address Proxy/Routers.

[0022] **FIG. 7** is an example flow diagram of an example routine provided by a DNS'/API server of the Address Management Proxy System to return a public address that corresponds to a designated unique identifier.

[0023] **FIG. 8** is an example flow diagram of an example routine within an Address Proxy/Router of an example Address Management Proxy System that receives data.

DETAILED DESCRIPTION OF THE INVENTION

[0024] Embodiments of the present invention provide computer- and network-based methods and systems for two-way initiated, bi-directional communication with wireless devices using connection-based or connection-less protocols, such as, for example, TCP/IP and UDP/IP. Example embodiments provide an Address Management Proxy System ("AMPS"), which enables devices and systems connected to a public internet, such as the Internet, to initiate communication with and to send data to wireless devices connected to a private wireless network, without exposing the non-routable private addresses of these wireless devices.

[0025] In existing systems, data communication (communication on a data channel) between a wireless device that is connected to a private wireless network and a wired device connected to a public wired network (e.g., the Internet) can only be initiated by the wireless device. Some carriers have assigned fixed public IP addresses to wireless devices; however, the wireless devices need to then have client programs (e.g., a UDP stack) capability of receiving and handling the incoming communication packets. Moreover, these wireless devices are then part of a public wireless network and not a private wireless network. Since public IP addresses are becoming a scarcer commodity and currently expensive to service a network of multi-million devices, carriers cannot in a practical sense count on having a fixed public IP address for each device on its network. (Although movement to IPv6 will allow more addresses, the current IPv4 definitions are limited and the potential number of wireless users subscribing to larger carriers is very high. In some regions of the world, the current public address scheme is even more limited.) Further, such addressing capability would expose each device to further security risks, because each such device is part of a publicly accessible network and it becomes more difficult to implement and enforce security measures. Thus, assigning private IP addresses to devices is preferred in existing wireless networks over assigning fixed public IP addresses to devices. When wireless networks are private, the locations (addresses) of the wireless devices are intentionally hidden from public view by a carrier system's (or, as referred to in some countries, operator's) infrastructure.

[0026] Wireless systems on private networks use techniques similar to Network Address Translation (NAT) technology to send data from a wireless device to the public networking world. In a typical carrier infrastructure that uses a private network, a wireless device "registers" itself with the carrier infrastructure when it powers on (or in other circumstances, when the device attempts to initiate data services). The carrier dynamically assigns the wireless device a private non-routable address by means of DHCP (or DHCP-like) server. The information on the mapping of the transient private IP address to the device public IP address is stored in an internal carrier database and managed by carrier services such as a RADIUS server.

[0027] The actual path taken by data when sent from a wireless device on a private network to the internet (or vice versa) is very much network infrastructure, carrier technology dependent, and proprietary. Although several standards have emerged, they are very diverse in nature. In a GPRS network, for example, a SGSN (Service GPRS node) manages the communication with wireless devices; whereas the SGSN connects to a GGSN (Gateway GPRS Node) to connect to the Internet network. Regardless of the mobile network used, data communication between a wireless device and internet involves various network elements like GGSN (or similar elements, based on GPRS, GSM, CDMA or any other network), DNS servers, routers and gateways.

[0028] Limited facilities exist for sending short sequence messages from a wired device on a public network to a mobile device on a wireless network (with a private address), again dependent upon carrier and network technology. SMS (Short Message System) protocol defines a format for such messages, but doesn't provide any guidance for underlying structure or data transfer. In addition, such messages are of a fixed (very short) length and use a specialized channel for sending control information (a signaling channel), not a data channel.

[0029] Therefore, there is no existing mechanism for setting up a bi-directional communication channel to communicate with wireless devices that are connected via a private network to the carrier infrastructure using a standard addressing scheme. Nor, is there any mechanism for initiating the communication with such a wireless device from a device connected to a public network. Thus, embodiments of existing systems are not able to support any kind of programmatic "push" of data to wireless devices from wired devices that reside external to a carrier's infrastructure. In

addition, messages sent from the wireless device to a device on a public (wired) network cannot be directly responded to by the wired device, because the address of the wireless device contained in the message may no longer be valid. Moreover, it is not possible using these systems to provide over-the-air provisioning of applications and to send other code to a wireless device from a device external to the carrier infrastructure. Over-the-air provisioning and related techniques for dynamic provisioning and downloading applications to wireless devices are discussed in detail in U.S. application Ser. No. 09/997,402, entitled "Method and System for Maintaining and Distributing Wireless Applications, filed on Nov. 28, 2001. Thus, a mechanism for allowing an external device with a public IP address to initiate bi-directional communication with a wireless device is highly desirable.

[0030] The Address Management Proxy System achieves two way initiated bi-directional communication by implementing a modified DNS server and serving as a proxy/router for devices on the private wireless network as they interface to the public wired internetworking world. In summary, a pool of public addresses is maintained and dynamically distributed among active wireless devices as needed by the AMPS. **FIG. 2** is a block diagram of an example Address Management Proxy System used in bi-directional communication with a wireless device. The term "bi-directional" as used herein means that data paths and communication can flow in either direction between two endpoint systems. **FIG. 2** shows wired devices **201, 202,** and **203** connected to public network **210**. One skilled in the art will recognize that these devices could be connected to another private or public network, which is then connected by one or more wired devices to the public network **210**, yet still achieve the functionality discussed here. Any such variation provides equivalent functionality and is explicitly contemplated and presumed to be part of the present invention. On the wireless side, the AMPS **220**, acting in its capacity as a proxy (and router) for wireless devices, is shown both connected via wire to the public network **210** and via standard carrier infrastructure elements (not shown) to the wireless network **230**. It is presumed that the reader has a working knowledge of the elements of a carrier's infrastructure and the basic mechanisms for routing and mechanisms converting packets from a wired network to a wireless network. These may use analog or digital technology and may require protocol conversions in order to send the physical data and transmit it, for example through a satellite, ultimately to the wireless device. Detailed background information on wireless technology and wireless routing mechanisms is described in Stallings, W., *Wireless Communications and Networks,* Prentice Hall, N.J., 2002, which is herein incorporated by reference in its entirety. In **FIG. 2**, wireless device **240** is shown connected via various wireless elements (not shown) to the wireless network **230**.

[0031] In operation, when a wired device such as wired device **201**, desires to send data to wireless device **240**, the wired device needs first to determine a routable address location of the wireless device **240** on the public network **210**. However, as can be observed from **FIG. 2**, the wireless device **240** is not directly connected to the public network **210**. Thus, the wired device must use the Address Management Proxy System **220** to determine a routable (public) address to which to send the data destined for the wireless device **240**. To accomplish this task, the wired device **201** performs a query (for example, a modified DNS query) to locate a routable public address that corresponds to wireless device **240**. The Address Management Proxy System **220** receives the query and determines and assigns a public (routable) address from a pool of addresses, which address can be used as a destination address for data packets targeted to wireless device **240**. One should note that, although shown here as a DNA query, the Address Management Proxy System, as will be described further, modifies the DNS query implementation to handle wireless device technology, and/or provides an alternative API for determining a suitable routable address. Once the Address Management Proxy System **220** has returned a routable address to wired device **201**, the wired device **201** can send data to that address. The Address Management Proxy System **220** receives the data, converts formats and protocols, etc., as needed, and sends the converted data through the wireless network **230** to the wireless device **240**.

[0032] **FIG. 3** is an example block diagram of components of an example Address Management Proxy System. In one embodiment, the Address Management Proxy System (AMPS) comprises one or more modified DNS'/API servers **302**, one or more Address Proxy/Routers **305**, an Address Management Data Server **303** which manages a database or other repositories such as Address Management Data Repository **304**, and optionally a load balancer **301**. The DNS'/API servers **302** are either individually connected to a public network **310** or are connected to the load balancer **301** which is in turn connected to public network **310**. Similarly, each Address Proxy/Router **305** is also connected to the public network **310**, via the routable (public) address to which data from the external network **310** is sent that is destined for the wireless devices. The DNS'/API servers **302** are either modified implementations of a DNS server to add functionality necessary to communicate with wireless devices, or are servers that implement one or more specialized APIs, as will be described further below. The DNS'/API servers **302** use the Address Management Data Server **303** to assist in mapping a unique identifier (e.g., string name) for a wireless device to a public address on public network **310**. The pool of public addresses is also maintained by the Address Management Data Serve **303** and Data Repository **304**. The Address Management Data server **303** and Address Management Data Repository **304** may be implemented using existing database technology, for example, ODBC technology or, may be implemented as a structure such as a simple text file. One skilled in the art will recognize that any embodiment for storing a set of tables, data, lists, or mappings can be used. Each Address Proxy/Router **305** also uses the Address Management Data Server **303** or equivalent to create and update a series of routing tables that are used to assign public addresses to wireless devices as needed and to update the various mappings between public addresses and the non-routable (private) addresses of the wireless devices. The tables and mappings that are maintained on behalf of the DNS'/API servers **302** and the Address Proxy/Routers **305** by the Address Management Data Server **303** are described below with reference to **FIG. 6**.

[0033] Although the techniques of the AMPS are generally applicable to any a wired device communicating with a wireless device, the phrase "public network" (or "wired network") is used generally to imply any type of internetworked environment including a public network or a backbone that is somewhere down the line connected to one or

more private or public networks. In addition, although the examples described herein often refer to the Internet, one skilled in the art will recognize that the concepts and inventions described are applicable to other forms and embodiments of internetworking, including, for example ATM type networks. Thus, techniques of the present invention can also be used by one device on a first wireless network to communicate with another wireless device on a second network—each device ends up communicating with the Address Proxy/Router of the other network. This scenario is feasible because each wireless network (or its carrier infrastructure) is connected to a proxy/router that is also connected (via a public address) to a public network. In addition, although a public network is sometimes also referred to herein as a wired network, one skilled in the art will recognize that any network that exposes routable (public) addresses may be implied. Thus, a wireless network with unique public (and routable) address can also employ techniques of the present invention to perform bi-directional communication. Also, one skilled in the art will recognize that terms such as wireless device, phone, handheld, etc., are used interchangeably to indicate any type of wireless device that is capable of operating with the AMPS. In addition, terms may have alternate spellings which may or may not be explicitly mentioned, and one skilled in the art will recognize that all such variations of terms are intended to be included.

[**0034**] Example embodiments described herein provide applications, tools, data structures and other support to implement private to public address mappings over one or more wired and wireless networks to be used for bi-directional communication. One skilled in the art will recognize that other embodiments of the methods and systems of the present invention may be used for many other purposes, including to push information and/or data or code from a public network such as the Internet to a wireless device. In addition, although this description primarily refers to "data" as being sent via the networks, one skilled in the art will recognize that all types of data can be communicated using the techniques described herein including, but not limited to, text, graphics, audio, and video.

[**0035**] Also, in the following description, numerous specific details are set forth, such as data formats and code sequences, etc., in order to provide a thorough understanding of the techniques of the methods and systems of the present invention. One skilled in the art will recognize, however, that the present invention also can be practiced without some of the specific details described herein, or with other specific details, such as changes with respect to the ordering of the code flow.

[**0036**] **FIG. 4** is an example block diagram of a general purpose computer system for practicing embodiments of the Address Management Proxy System. The general purpose computer system **400** may comprise one or more server and/or client computing systems and may span distributed locations. In addition, each block may represent one or more such blocks as appropriate to a specific embodiment or may be combined with other blocks. The various blocks of the Address Management Proxy System **410** may physically reside on one or more machines, which use standard interprocess communication mechanisms to communicate with each other. In the embodiment shown, computer system **400** comprises a computer memory ("memory") **01**, a display **402**, a Central Processing Unit ("CPU") **403**, and Input/Output devices **404**. The Address Management Proxy System **410** is shown residing in memory **401**. The components of the Address Management Proxy System **410** preferably execute on CPU **403** and manage the address mapping of wireless devices on a wireless network, as described in previous figures, to allow other wired systems to communicate with the wireless devices. Other downloaded code **405** and potentially other data repositories also reside in the memory **410**, and preferably execute on one or more CPU's **403**. In a typical embodiment, the AMPS **410** includes one or more DNS'/API servers **411**, one or more Address Proxy/Routers **412**, an Address Management Data Server **413**, and Address Management Data Repositories **414**. As described earlier, the AMPS may include other data repositories and components, such as a load balancer, depending upon the particular implementation.

[**0037**] In an example embodiment, components of the AMPS **410** are implemented by modifying existing UDP-based technology, such as DNS servers and routers, which are typically implemented on Linux/Unix systems written in the C programming language. Programming interfaces to the DNS'/API servers **411** and Address Proxy/Routers **412** can be available by standard means such as through C, C++, C#, and Java API and through scripting languages such as XML, or through web servers supporting such. The Address Management Data Server **413** and Address Management Data Repositories **414** are preferably implemented for scalability reasons as a database system rather than as a text file and may be implemented using a SQL/ODBC database management system. The DNS'/API servers **411** and Address Proxy/Routers **412** are typically implemented using Linux, UNIX, or other Unix-based or Unix-like machines.

[**0038**] One skilled in the art will recognize that the AMPS **410** may be implemented in a distributed environment that is comprised of multiple, even heterogeneous, computer systems and networks. For example, in one embodiment, the DNS'/API servers **411**, the Address Proxy/Router components **412**, and the Address Management Data Servers **413** with their data repositories **414** are all located in physically different computer systems. In another embodiment, various components of the AMPS **410** are hosted each on a separate server machine and may be remotely located from the tables which are stored in the address management data repository **414**. In addition, under some scenarios, the entire AMPS system **410** may be hosted within a carrier's infrastructure and be completely subsumed by it. Different configurations and locations of programs and data are contemplated for use with techniques of the present invention. In example embodiments, these components may execute concurrently and asynchronously; thus the components may communicate using well-known message passing techniques. One skilled in the art will recognize that equivalent synchronous embodiments are also supported by an AMPS implementation. Also, other steps could be implemented for each routine, and in different orders, and in different routines, yet still achieve the functions of the AMPS.

[**0039**] There are several implementation approaches to the components of the Address Management Proxy System, three of which are described herein. One skilled in the art will recognize that various other approaches and combinations are possible. All three approaches allocate a public (routable) network address for temporary use by a wired

device to communicate with a wireless device. In one embodiment, a pool of public addresses, for example, public IP addresses, is maintained and allocated dynamically to wireless network devices as required. For example, a typical Class B Internet network address block allows for approximately 65,000 simultaneous connections to wireless devices. Although this number may seem large at first blush, when one considers the number of cell phones and handsets, for example, connected to a carrier, this number can be quite limiting.

[0040] The first approach provides a public address mapping for a wireless device and makes it available using a UDP protocol. This is a store and forward type of approach. One advantage of this approach is that it facilitates UDP-based traffic to wireless devices over a wireless connection and allows a device connected to the public side of the connection to initiate the connection. A disadvantage, however, is that either the standard UDP protocol requires modification or an extra API call is added so that the requesting device can identify the destined wireless device. These modifications are necessary because the UDP protocol only supports the designation of an IP address and does not provide for an alternative means of uniquely identifying a device (such as a string similar to the TCP/IP protocol). Since it is desirable to hide this (private) address, the standard UDP call to send data does not suffice.

[0041] The second approach used to implement the AMPS supports full bi-directional communication through point-to-point connections established, for example, using TCP/IP protocol. (Note that these same techniques also support connection-less UDP bi-directional communication). The second approach can be implemented by providing a modified implementation of a standard UDP or TCP/IP function, "GetHostByName." The GetHostByName API allows a string designation to identify the designated device and returns an IP address data structure. Alternatively, to increase the level of security provided, the AMPS can implement a specialized API to return the dynamically allocated public address that (now) corresponds to the requested wireless device. A disadvantage of the specialized API approach is that the device on the public network (or other device that wishes to obtain a connection to the wireless device) needs to include specialized code in the application on the requesting device.

[0042] The third approach is similar to the second approach, but provides for greater potential simultaneous connections using a "port" concept. Using this approach, instead of returning just a host address on the wired network that corresponds to the wireless device (a public address of an Address Proxy/Router), the AMPS also returns a particular port designation on the host machine (the Address Proxy/Router). Ports and their implementation are well known in the art and, in general, correspond to queues implemented by the machine that receives the data to track messages destined for different locations. The machines that receive the data forward messages to the different destinations based upon the port designations in the message and handle, where necessary, sequencing and handshaking on a by-port basis.

[0043] Ports are typically used to open multiple virtual channels on a single physical address and potentially extend a single physical address to another approximately 65,000 connections. This enables an AMPS to use Class C IP addresses, for example, which are typically much cheaper and more readily available than the other types of addresses, to achieve approximately 16 million simultaneous connections to wireless devices (using a UNIX-based system). One skilled in the art will recognize that the number of ports available and their particular implementation is operating system dependent and directly correlates to the number of bits used to specify a port address.

[0044] The UDP (as well as TCP/IP) protocol currently supports a port abstraction; however, the standard DNS query used with UDP and TCP/IP systems (e.g., GetHostByName) does not allow for the returning of a port designation and leaves control of the port designation up to the requesting device instead of the receiving router. Thus, according to the third approach to implementing the AMPS, ports are specified preferably by the Address Proxy/Router using a specialized API and returned to the requesting device with the host machine designation.

[0045] In one embodiment, a scripting language interface, such as XML, can be used instead of a specialized API (code interface) to interface to a specialized address mapping function. When using XML, the DNS'/API server accepts API calls as XML post events and returns XML formatted responses. Similar support for invoking this mapping function using other language models and/or other programming languages is also contemplated and will operate with techniques of the present invention. An XML type interface minimizes the cost to a requesting device of integrating an API into its software.

[0046] In addition, when using a specialized API, the requesting device can push additional data to the private wireless device with no further coding effort required. For example, billing code orienting to billing the wireless device for the type of connection being established with the wired device can be pushed to the wireless device using this technique. An example billing code mechanism is discussed in U.S. patent application Ser. No. 10/085,981, entitled "Method and System for Transmission-Based Billing of Applications," filed on Feb. 26, 2002.

[0047] There are several security related reasons that also may indicate a desire to use a specialized API rather than the standard GetHostByName API of UDP and TCP/IP. These security reasons may indicate a desire to use the port-based mechanism which also requires a specialized API. First, any bi-directional communication that uses the "GetHostByName" API and router protocol is susceptible to denial of service (DOS) attacks associated with that host name. DOS attacks can occur as a result of one or more machines specifying the same GetHostByName with the same input parameter simultaneously so as to close out the possibility of enough public addresses (of proxy/router machine addresses) being available. Second, use of the GetHostByName (or any other standard) API also makes the AMPS susceptible to security attacks as a result of DNS zone transfer. DNS zone transfer occurs, for example, when one DNS transfers a DNS query to one or more other DNS servers in order to find a requested host name. One typical scenario involves multiple DNS hops from country to country. The idea of DNS zone server attacks is to capture information on a particular DNS server by inserting malicious code as a malicious DNS server and impersonate the

AA/SWA Ex. 1015, p.75 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

destination address. Third, inattentiveness to the duration of a connection can make data available to unauthorized requesting devices. Specifically, since a mapping is established between the public device and a wireless device, the public device may assume the mapping to exist longer than it really does and potentially end up (maliciously or not) communicating with the wrong device. This could occur because some DNS server implementations ignore Time to Live settings. Having a modified DNS server implementation, whether or not it implements the standard GetHostByName API, or a specialized API, avoids this problem by abiding by the TTL characteristics of the established mapping between the private and the public addresses.

[0048] FIGS. **5-8** describe various example embodiments of the specific routines implemented by the DNS'/API servers and the Address Proxy/Routers to achieve the functionality described with reference to **FIGS. 2 and 3**. **FIG. 5** is an example flow diagram of the process performed by a device on a public network to send data to a wireless device located on a private wireless network using the Address Management Proxy System. In step **501**, the source (e.g., wired) device requests a public (routable) address for the designated wireless device from the AMPS. As described above, one mechanism for retrieving such an address is for the AMPS to implement a modified interface for DNS services, such as a modified GetHostByName routine. For example, a GetIIostByName routine may be invoked to specify a unique wireless device designation, in a string form. The string "personname.phone.wsp.com" is an example string that indicates a wireless device that corresponds to a person by the name of "person," with a phone number of "phone," located at a wireless service provider's website (DNS) that is abbreviated "wsp.com." (For example, susan.ph2065551212.sprint.com may refer to a person, Susan, with phone number 206 555 1212, on a sprint network.) Another mechanism that may be implemented by the AMPS is to provide a separate (specialized) API, such as "GetProxyIP" which returns an indication of a public (routable) address that corresponds to the designated wireless device. Using a separate API is useful for security reasons; for example, it becomes more difficult for a rogue device to intercept the routable address by spoofing. Another reason is to control the actual format of the address information returned, such as to be able to provide a port designation in addition to a host address of the Address Proxy/Router. The implementation of either GetHostByName, or a specialized API such as GetProxyIP, is discussed further below with respect to **FIG. 7**.

[0049] In step **502**, once the public address for the wireless device has been returned by the AMPS, the source device extracts from the indicated address information an actual address location (IPdata.ip), a Time to Live parameter (IPdata.TTL), and optionally, where applicable, a port designation (IPdata.port) for example, when the standard GetHostByName API is not used. In step **503**, when the source device desires to perform connection-based communication with the wireless device, it opens a connection, such as a socket. In step **504**, the wired device determines whether the Time to Live parameter specifies that the returned public address of the wireless device has expired, and, if so, returns to step **501** to request a different address, else continues in step **505**. The Time to Live parameter is used by the AMPS to ensure that a public address for a wireless device (which may or may not be always connected to the wireless network and powered on) does not extend past a period of usefulness for that wireless device. In some embodiments, a very short TTL parameter is used, to prevent security breaches in which a wired device is able to monitor activity on a particular public address and then use that address for other purposes. In step **505**, the wired device sends a data packet (via the connection or not) to the wireless device. It is presumed, but not shown, that the wired device and the wireless device communicate using the standard calls specified in the transfer protocol being used, for example UDP or TCP/IP. In step **506**, if the data transaction is complete, then the wired device is done, else it returns to check the TTL parameter in step **504** in order to send more data.

[0050] Table 1 below contains pseudocode that describes one example implementation of how a public (requester) device can use a modified GetHostByName query as described in **FIG. 5** to obtain a public address that corresponds to a user identified by the phone number "2065551212" using the Address Management Proxy System. From the public device's perspective, standard UDP and TCP/IP calls are invoked in a standard manner.

TABLE 1

```
InetAddress ip =
InetAddress.GetHostByName("2065551212.fourthDNs.att.com");
byte [] data;
int destPort = 80;
// data buffer filled by some internal routine say
// popuiateDataBuffer(), which in turn uses setData() Java
API.
int datasize = populateDataBuffer(data);
DatagramSocket socket = new DatagramSocket(destPort, ip);
// Now send some data . . .
DatagramPacket packet = new DatagramPacket (data,
datasize);
socket.send (pncket);
```

[0051] Table 2 below contains pseudocode that describes an example implementation of the specialized API mechanism described in **FIG. 5** as used by a public (requester) device to obtain a public address of the user identified by the same phone number. In Table 2, the public device calls a specialized API, GetProxyIP, to get a data structure that contains the needed information including the assigned public address of the Address Proxy/Server. Thereafter, the public device can use the same techniques (standard UDP or TCP/IP protocol) to send the data.

TABLE 2

```
public class IPInfo
{
    private String _publicIPAddress;
    private int _publicPort, _TTL;
    public String getPublicIPAddress()  {
        return _publicIPAddress;
    }
    public int getPublicPort()  {
        return_publicPort;
    }
    public int getTTI.()
    {
        return _TTL;
    }
}
int destPort = 80;
IPInfo ipi = GetProxyIP("2065551212.fourthDNS.att.com",
```

TABLE 2-continued

```
destPort);
// Return value of ipi.getPublicIPAddress() in format
x.y.z.q
// For example: 142.432.14.2
InetAddress ip =
InetAddress.getByName (ipi.getPublicIPAddress ());
byte [] data;
// data buffer filled by some internal routine say
// populateDataBuffer(), which in turn uses setData()
Java API.
int datasize = populateDataBuffer(data);
DatagramSocket socket =
      new DatagramSocket (destPort, ipi.getPublicPort ());
// Now send some data. . .
DatagramPacket packet = new DatagramPacket (data,
datasize);
socket.send (packet)
```

[0052] **FIG. 6** is an example block diagram of some of the Address Management Proxy System data repository tables used to support routines of the DNS'/API servers and the Address Proxy/Routers. In one embodiment, the Address Management Data Repository comprises three tables: a unique identifier (unique ID) to private address table **610**, a public-to-private address table **630**, and a public address to proxy/router machine table **620**. Although three tables are shown, one skilled in the art will recognize that these tables could contain other data and may be organized differently, including a different number of tables and with different columns or fields. In addition, any technique for storing a table or list of data may be used. To support embodiments that map a host address plus a port designator to a wireless device, the tables are correspondingly modified.

[0053] The unique ID table **610** maps unique string names of wireless devices to the private wireless network addresses that have been assigned typically by a carrier's infrastructure. In some embodiments, the carrier infrastructure dynamically allocates, using methods similar to a DHCP protocol, a private wireless network address when the wireless device registers itself with the carrier infrastructure upon being powered on. Thus, the unique ID table **610** may be sparsely filled or entries created dynamically and then deleted dynamically as devices register and unregister with the carrier infrastructure system.

[0054] The public-to-private address table **630** comprises several fields/columns including a public network address **631**, a private (wireless) network address **602**, a flag **632** that specifies whether the public address stored in field **631** is free or is already used, a Time to Live (TTL) parameter **633**, and other connection data **634**. In one embodiment, the DNS'/API servers of the AMPS query table **630** to determine a public network address that corresponds to a designated private wireless network address or to allocate an unused public network address (as indicated in field **632**) and map the determined unused public address to a private network address stored in field **602**.

[0055] Public address to proxy/router machine table **620** comprises a public network address field **631** and an indication of a functioning proxy/router machine **621**. By maintaining such a mapping, the AMPS is able to substitute proxy/router machines for other proxy/router machines to provide a higher degree of robustness. Each proxy/router machine has a preconfigured set of public network addresses, such as are typically configured by network cards inserted into the proxy/router machine. These address are allocated in a standard fashion through prior purchase or obtaining from an address authorizing authority, currently the Internet Corporation for Assigned Names and Numbers (ICANN). When a machine is inserted for use into the AMPS, indications of these addresses are stored in field **631**.

[0056] In one embodiment, a timestamp of the mapping between a public network address and a private address is also noted in table **630**. After a defined time out, based upon this timestamp, the Address Management Data Server sends a request to the Address Proxy/Router associated with the mapping to unmap the public-to-private address mapping and updates the mapping table **630**, thereby returning the associated public address to the pool of unused public network addresses.

[0057] **FIG. 7** is an example flow diagram of an example routine provided by a DNS'/API server of the Address Management Proxy System to return a public address that corresponds to a designated unique identifier. In essence, this routine implements a DNS query or DNS-like query capability for the AMPS using a modified GetHostByName interface or a specialized API, for example GetProxyIP, as described with reference to **FIG. 5**. In summary, the routine dynamically allocates an appropriate Address Proxy/Router machine to associate with the wireless device and returns the public address of that machine (along with a TTL parameter and potentially other parameters). Specifically, in step **701**, the routine determines the private (non-routable) address of the wireless device designated by a string parameter passed as input to the routine. For example, the string parameter may use fields such as "uniqueID.hostname.domain.tld," which specifies a typical hierarchy of person/service on a machine named "hostname" on a domain such as a company's network on a top level domain such as "org.""com,""edu," etc. One skilled in the art will recognize that many other string parameter designations could be used. One mechanism for implementing this routine is to request information from the Address Management Data Repository. In one embodiment, the data repository stores a table that maps unique IDs to private network addresses (see Table **610** in **FIG. 6**). Preferably, any mechanism that is used by the AMPS stores this data in a secure manner in order to keep the wireless network addresses private. In step **702**, the routine retrieves the public network address that corresponds to the private wireless network address of the designated device if one has already been assigned by the AMPS to that device and is still valid. In one embodiment, the data repository stores this mapping information between private wireless network address and public network address (see for example table **630** in **FIG. 6**). If a public network address has not already been assigned or is not valid, then the routine causes a new public network address to be allocated and that new public address is associated with the private wireless network address. Appropriate tables in the data repository are then updated. In step **703**, the routine determines the Address Proxy/Router machine that is associated with the assigned public network address (for example using table **620** in **FIG. 6**). In step **704**, the routine sends a request to the determined proxy/router machine to update its routing tables to map the determined public network address to the private wireless network address. In step **705**, the routine updates information in the data repository to include any other

AA/SWA Ex. 1015, p.77 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

connection related information (e.g., field **634** in Table **630** in **FIG. 6**) and indicates a Time to Live (TTL) parameter for the public-private address association (e.g., field **633** in Table **630** in **FIG. 6**). Once all of the tables have been updated in both the proxy/router and in the data repository, the DNS'/API server returns the determined public network address of the associated Address Proxy/Router machine. As described earlier, the public address may be a (hostname, port) pair when a port-based implementation is used.

[0058] **FIG. 8** is an example flow diagram of an example routine within an Address Proxy/Router of an example Address Management Proxy System that receives data. This routine is implemented by an Address Proxy/Router to receive data from wired devices using the relevant protocol (e.g., TCP/IP, UDP/IP, etc.). (Data is sent to a particular Address Proxy/Router because the public (routable) address of that Address Proxy/Router was returned to the requesting/source device in response to a query of the DNS'/API server of the AMPS.) The proxy/router is responsible for any conversions of the data necessary to send data from the wired network to the wireless network (if, for example, the carrier infrastructure desires such conversion to be performed at this level). The proxy/router is also responsible for forwarding the data via the wireless network to the private wireless address of the wireless device that corresponds to the public address used to invoke the proxy/router.

[0059] Specifically, in step **801**, the routine determines (for example, from the Address Management Data Repository) the private wireless address that corresponds to the invoked public address and the TTL parameter associated with this mapping. These values can be obtained, for example, from the public-to-private address table **630** of **FIG. 6**. In step **802**, the routine determines whether the value of the determined TTL parameter indicates that the mapping has expired, and if so, returns an error, else continues in step **803**. In step **803**, the routine determines the format required by the target device (the wireless network format). In step **804**, the routine determines whether any protocol conversion is necessary and, if so, continues in step **805** else continues in step **806**. Note that protocol conversion for a specific wireless network such as converting the data to an "HTTP" packet may be done by the proxy/router or may be done by some other component within the carrier infrastructure. One skilled in the art will recognize that these are example steps and that different formatting or different protocol conversion routines may be added or omitted as specific to the environment. In step **806**, the Address Proxy/Router routine sends the data packet (which has been formatted and whose protocol is converted as necessary) to the determined associated private address of the wireless device, and returns.

[0060] All of the above U.S. patents, U.S. patent application publications, U.S. patent applications, foreign patents, foreign patent applications and non-patent publications referred to in this specification and/or listed in the Application Data Sheet, including but not limited to U.S. Provisional Patent Application No. 60/296,902, entitled "Method and System for Two-Way Initiated Data Communication with Wireless Devices," filed Jun. 8, 2001; U.S. patent application Ser. No. 09/997,402, entitled "Method and System for Maintaining and Distributing Wireless Applications," filed Nov. 28, 2001; and U.S. patent application Ser. No. 10/085,981, entitled "Method and System for Transmission-Based Billing of Applications," filed on Feb. 26, 2002 are incorporated herein by reference, in their entirety.

[0061] From the foregoing 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 deviating from the spirit and scope of the invention. For example, one skilled in the art will recognize that the methods and systems for establishing bi-directional communication discussed herein are applicable to other types of public networks and protocols other than the Internet, TCP/IP, and UDP, or even a plurality of such networks. For example, private address to public address mappings can also be provided for ATM networks to connect devices on an ATM network with a wireless device. One skilled in the art will also recognize that the methods and systems discussed herein are applicable to differing protocols, communication media (optical, wireless, cable, etc.) and wireless devices (such as wireless handsets, electronic organizers, personal digital assistants, portable email machines, game machines, pagers, navigation devices such as GPS receivers, etc.) to different wired device (such as kiosks, personal computers, mainframes), and to wireless devices having a wired connection capabilities, e.g., wireless email or PDA devices that can be connected to a docking station for synchronization purposes.

1. A method in a computer network environment that is connected to a wireless communications network through an address management proxy system, the wireless communications network connected to a wireless device using a private network address of the wireless communications network, the wireless device having an associated unique identifier, the address management proxy system having a public network address of the computer network environment, and the computer network environment connected to a wired device using a public network address of the computer network environment, comprising:

under control of the wired device,

using the public network address of the address management proxy system, sending a request to the address management proxy system for an indication of a public network address of the computer network environment to use for communicating with the wireless device, the request indicating the unique identifier associated with the wireless device;

under control of the address management proxy system,

receiving the request for the indication of the public network address;

determining a public network address from a plurality of available public network addresses of computer network environment;

associating the determined public network address with the private network address of the wireless device that corresponds to the indicated unique identifier; and

forwarding an indication of the determined public network address to the wired device; and

under control of the wired device,

receiving the indicated public network address; and

sending data to the wireless device using the indicated public network address, such that the wired device perceives that the wired device is communicating directly with the wireless device.

2. The method of claim 1, further comprising:

under control of the address management proxy system,

receiving the data sent from the wired device;

determining the private network address that is associated with the indicated public network address; and

routing the received data to the private network address over the wireless communication network in a manner that is transparent to the wired device.

3. The method of claim 1 wherein the computer network environment is the Internet and each public network address is specified in accordance with Internet Protocol (IP) addressing conventions.

4. The method of claim 1 wherein the computer network environment is an ATM network.

5. The method of claim 1 wherein the indicated public network address is the public network address of the address management proxy system, wherein data sent from the wired device indicates the unique identifier of the wireless device, and wherein the address management proxy system stores and forwards the data to the wireless device associated with the indicated unique identifier.

6. The method of claim 1 wherein the indicated public network address is received as a result of a call by the wired device to an address mapping function of the computer network environment.

7. The method of claim 6 wherein the address mapping function is a standard function of the computer network environment.

8. The method of claim 6 wherein the address mapping function is a GetHostByName function.

9. The method of claim 1 wherein the indicated public network address is received as a result of a call by the wired device to a function that returns a host system address and a port specification.

10. The method of claim 9 wherein the function is a customized API.

11. The method of claim 9 wherein the function supports an XML interface.

12. The method of claim 1, further comprising:

under control of the wireless device, sending data to the wired device using the public network address of the wired device, thereby performing bi-directional communication.

13. The method of claim 1 wherein a virtual end-to-end connection is established between the wired device and the wireless device.

14. The method of claim 1 wherein a connectionless communications path is established between the wired device and the wireless device.

15. A computer network environment comprising:

a wireless device connected to a wireless communications network using a private network address of the wireless communications network, the wireless device having an associated unique identifier;

a wired device connected to the computer network environment using a public network address of the computer network environment, that is structured to:

request an indication of a public network address of the computer network environment to use for communicating with the wireless device, the request indicating the unique identifier associated with the wireless device,

receive the indicated public network address, and,

send data to the wireless device using the indicated public network address, such that the wired device communicates directly with the wireless device using a virtual end-to-end connection; and

an address management proxy system connected to the computer network environment using a public network address of the computer network environment, that is structured to:

receive the request from the wired device,

determine a public network address from a plurality of available public network addresses of computer network environment,

associate the determined public network address with the private network address of the wireless device that corresponds to the indicated unique identifier, and

forward an indication of the determined public network address to the wired device.

16. The computer network environment of claim 15 wherein the address management proxy system is further structured to:

receive the data sent from the wired device,

determine the private network address that is associated with the indicated public network address, and

route the received data to the private network address over the wireless communication network in a manner that is transparent to the wired device.

17. The computer network environment of claim 15 wherein the computer network environment is the Internet and each public network address is specified in accordance with Internet Protocol (IP) addressing conventions.

18. The computer network environment of claim 15 wherein the computer network environment is an ATM network.

19. The computer network environment of claim 15 wherein the indicated public network address is the public network address of the address management proxy system, wherein data sent from the wired device indicates the unique identifier of the wireless device, and wherein the address management proxy system is structured to store and forward the data to the wireless device associated with the indicated unique identifier.

20. The computer network environment of claim 15 wherein the indicated public network address is received as a result of a call by the wired device to an address mapping function of the computer network environment.

21. The computer network environment of claim 20 wherein the address mapping function is a standard function of the computer network environment.

22. The computer network environment of claim 20 wherein the address mapping function is a GetHostByName function.

23. The computer network environment of claim 15 wherein the indicated public network address is received as a result of a call by the wired device to a function that returns a host system address and a port specification.

24. The computer network environment of claim 23 wherein the function is a customized API.

25. The computer network environment of claim 23 wherein the function supports an XML interface.

26. The computer network environment of claim 15, wherein the wireless device is further structured to send data to the wired device using the public network address of the wired device, thereby performing bi-directional communication.

27. The computer network environment of claim 15 wherein a virtual end-to-end connection is established between the wired device and the wireless device.

28. The computer network environment of claim 15 wherein a connectionless communications path is established between the wired device and the wireless device.

29. A method in a computer network environment for establishing a bi-directional communication channel virtual communication channel between a first device connected to the computer network environment using a public network address and a second device connected to a wireless communications network and having a private address, comprising:

receiving a request from the first device to communicate with the second device;

dynamically determining a public network address from a pool of public network addresses;

associating the determined public network address with the private address of the second device; and

returning an indication of the determined public network address to the first device so that the first device can thereafter send data to the second device using the determined public network address.

30. The method of claim 29 wherein the request indicates a unique identifier of the second device that is different from the private address of the second device, and the associating the determined public address with the private address of the second device is performed using the unique identifier.

31. The method of claim 29, further comprising:

receiving data from the first device directed to the determined public network address; and

transparently routing the received data to the second device using the private network address associated with the determined public network address.

32. The method of claim 31 wherein the transparent routing is performed by a masquerading system connected to the computer network environment by a public network address of the computer network environment.

33. The method of claim 29 wherein the first device is a wired device.

34. The method of claim 29 wherein the first device is a wireless device.

35. The method of claim 29 wherein the second device is a device capable of a wired connection.

36. The method of claim 29 wherein the second device is a wireless device.

37. The method of claim 29 wherein the determined public network address specifies a host system address and a port specification.

38. The method of claim 29 wherein the determined public network address specifies an Internet Protocol (IP) address.

39. The method of claim 29 wherein the method is performed by a modified DNS server.

40. The method of claim 29 wherein the received request is a standard API of the computer network environment.

41. The method of claim 40 wherein the API is a GetHostByName API.

42. The method of claim 29 wherein the received request is a modified API of the computer network environment that specifies a name of a host machine and an indication of a port.

43. The method of claim 29, further comprising:

associating the determined public network address with an expiration period; and

destroying the association between the determined public network address and the private address of the second device when the expiration period as expired.

44. The method of claim 43 wherein the expiration period is specified as Time to Live (TTL) data.

45. An address proxy management system connected to a computer network environment for establishing a virtual communication channel between a first device connected to the computer network environment using a public network address and a second device connected to a wireless communications network and having a private address comprising:

domain name service (DNS) that is structured to:

receive a request from the first device to communicate with the second device,

dynamically determine a public network address from a pool of public network addresses;

associate the determined public network address with the private address of the second device; and

return an indication of the determined public network address to the first device so that the first device can thereafter send data to the second device using the determined public network address.

46. The system of claim 45 wherein the DNS is a modified DNS that abides by at least one of UDP and TCP/IP standards.

47. The system of claim 45 wherein the computer network environment is the Internet.

48. The system of claim 45 wherein each public network address is specified in accordance with Internet Protocol (IP) addressing conventions.

49. The system of claim 45 wherein the DNS uses a database to associate the determined public network address with the private address of the second device.

50. The system of claim 45 wherein the DNS uses a database to dynamically determine a public network address from a pool of public network addresses.

51. The system of claim 45 wherein the request indicates a unique identifier of the second device that is different from the private address of the second device, and the DNS associates the determined public address with the private address of the second device using the unique identifier.

52. The system of claim 45, further comprising:

private address management router that is structured to receive data from the first device directed to the determined public network address, and transparently routes the received data to the second device using the private network address associated with the determined public network address.

53. The system of claim 52 wherein the private address management router is connected to the computer network environment by a public network address of the computer network environment, and transparently routes the received data to the public address of the second device by determining the private network address associated with the received data and causes the data to be forwarded over the wireless communications network to the second device at the determined private network address.

54. The system of claim 52 wherein the private address management router causes protocol conversion of the received data to be performed when applicable before transparently routing the received data.

55. The system of claim 45 wherein the first device is a wired device.

56. The system of claim 45 wherein the first device is a wireless device.

57. The system of claim 45 wherein the second device is a device capable of a wired connection.

58. The system of claim 45 wherein the second device is a wireless device.

59. The system of claim 45 wherein the determined public network address specifies a host system address and a port specification.

60. The system of claim 45 wherein the determined public network address specifies an Internet Protocol (IP) address.

61. The system of claim 45 wherein the received request is a standard API of the computer network environment.

62. The system of claim 61 wherein the API is a GetHostByName API.

63. The system of claim 45 wherein the received request is a new API that specifies a name of a host machine and an indication of a port.

64. The system of claim 45, wherein the DNS is further structured to:

associate the determined public network address with an expiration period; and

cause the association between the determined public network address and the private address of the second device to be destroyed when the expiration period as expired.

65. The system of claim 64 wherein the expiration period is specified as Time to Live (TTL) data.

66. An address proxy management system connected to a computer network environment for establishing a virtual communication channel between a first device connected to the computer network environment using a public network address and a second device connected to a wireless communications network and having a private address comprising:

means for receiving a request from the first device to communicate with the second device;

means for dynamically determining a public network address from a pool of public network addresses;

means for associating the determined public network address with the private address of the second device; and

means for returning an indication of the determined public network address to the first device so that the first device can thereafter send data to the second device using the determined public network address.

67. A computer-readable memory medium containing instructions for controlling a processor in a computer system to establish a bi-directional communication channel virtual communication channel between a first device connected to a computer network environment using a public network address and a second device connected to a wireless communications network and having a private address, by:

receiving a request from the first device to communicate with the second device;

dynamically determining a public network address from a pool of public network addresses;

associating the determined public network address with the private address of the second device; and

returning an indication of the determined public network address to the first device so that the first device can thereafter send data to the second device using the determined public network address.

68. The computer-readable memory medium of claim 67 wherein the request indicates a unique identifier of the second device that is different from the private address of the second device, and the associating the determined public address with the private address of the second device is performed using the unique identifier.

69. The computer-readable memory medium of claim 67, the instructions further controlling the computer processor by:

receiving data from the first device directed to the determined public network address; and

transparently routing the received data to the second device using the private network address associated with the determined public network address.

70. The computer-readable memory medium of claim 69 wherein the transparent routing is performed by a masquerading system connected to the computer network environment by a public network address of the computer network environment.

71. The computer-readable memory medium of claim 67 wherein the first device is a wired device.

72. The computer-readable memory medium of claim 67 wherein the first device is a wireless device.

73. The computer-readable memory medium of claim 67 wherein the second device is a device capable of a wired connection.

74. The computer-readable memory medium of claim 67 wherein the second device is a wireless device.

75. The computer-readable memory medium of claim 67 wherein the determined public network address specifies a host system address and a port specification.

76. The computer-readable memory medium of claim 67 wherein the determined public network address specifies an Internet Protocol (IP) address.

77. The computer-readable memory medium of claim 67 wherein the method is performed by a modified DNS server.

78. The computer-readable memory medium of claim 67 wherein the received request is a standard API of the computer network environment.

79. The computer-readable memory medium of claim 78 wherein the API is a GetHostByName API.

80. The computer-readable memory medium of claim 67 wherein the received request is a modified API of the computer network environment that specifies a name of a host machine and an indication of a port.

81. The computer-readable memory medium of claim 67, the instructions further controlling the computer processor by:

associating the determined public network address with an expiration period; and

destroying the association between the determined public network address and the private address of the second device when the expiration period as expired.

82. The computer-readable memory medium of claim 81 wherein the expiration period is specified as Time to Live (TTL) data.

83. A method in a computer network environment for communicating with a wireless device connected to an address management proxy system using a private network address, the wireless device having an associated unique identifier that is not the private network address, the address management proxy system connected to the computer network environment using a public network address of the network environment, comprising:

requesting from the address management proxy system a public network address that corresponds to the unique identifier associated with the wireless device;

receiving an indication of the public network address of the wireless device; and

sending data to the indicated public network address.

84. The method of claim 83 wherein the computer network environment is the Internet.

85. The method of claim 83 wherein the indicated public network address is specified in accordance with Internet Protocol (IP) addressing standards.

86. The method of claim 83 wherein the unique identifier is at least one of a person's name and telephone number, an MSISDN number, and an ISMI number.

87. The method of claim 83 wherein the request is a standard API, such that communication with the wireless device is performed in the same manner as communication with a wired device connected to the computer network environment.

88. The method of claim 87 wherein the API is a GetHostByName function call.

89. The method of claim 83 wherein the indication of the public network address of the wireless device is a host machine address.

90. The method of claim 83 wherein the indication of the public network address of the wireless device is a host machine address and a port specification.

91. A computer-readable memory medium containing instructions for controlling a computer processor to communicate in a computer network environment with a wireless device connected to an address management proxy system using a private network address, the wireless device having an associated unique identifier that is not the private network address, the address management proxy system connected to the computer network environment using a public network address of the network environment, by:

requesting from the address management proxy system a public network address that corresponds to the unique identifier associated with the wireless device;

receiving an indication of the public network address of the wireless device; and

sending data to the indicated public network address.

92. The computer-readable memory medium of claim 91 wherein the computer network environment is the Internet.

93. The computer-readable memory medium of claim 91 wherein the indicated public network address is specified in accordance with Internet Protocol (IP) addressing standards.

94. The computer-readable memory medium of claim 91 wherein the unique identifier is at least one of a person's name and telephone number, an MSISDN number, and an ISMI number.

95. The computer-readable memory medium of claim 91 wherein the request is a standard API, such that communication with the wireless device is performed in the same manner as communication with a wired device connected to the computer network environment.

96. The computer-readable memory medium of claim 95 wherein the API is a GetHostByName function call.

97. The computer-readable memory medium of claim 91 wherein the indication of the public network address of the wireless device is a host machine address.

98. The computer-readable memory medium of claim 91 wherein the indication of the public network address of the wireless device is a host machine address and a port specification.

99. A wired device that is connected to a computer network environment using a public network address of the computer network environment, the network environment connected to an address management proxy system using a public network address of the network environment, the address management proxy system connected to a wireless device using a private network address, the wireless device having an associated unique identifier that is not the private network address, comprising:

communications code module that is structured to:

request from the address management proxy system a public network address that corresponds to the unique identifier associated with the wireless device,

receive an indication of the public network address of the wireless device; and

send data to the indicated public network address.

100. The device of claim 99 wherein the computer network environment is the Internet.

101. The device of claim 99 wherein the indicated public network address is specified in accordance with Internet Protocol (IP) addressing standards.

102. The device of claim 99 wherein the unique identifier is at least one of a person's name and telephone number, an MSISDN number, and an ISMI number.

103. The device of claim 99 wherein the request is a standard API, such that communication with the wireless device is performed in the same manner as communication with a wired device connected to the computer network environment.

AA/SWA Ex. 1015, p.82 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

104. The device of claim **103** wherein the API is a GetHostByName function call.

105. The device of claim 99 wherein the indication of the public network address of the wireless device is a host machine address.

106. The device of claim 99 wherein the indication of the public network address of the wireless device is a host machine address and a port specification.

107. The device of claim 99 wherein the communications code module implements at least one of UDP and TCP/IP communication with the wireless device.

108. The device of claim 99 wherein the communications code module implements UDP communication with the wireless device.

* * * * *

EXHIBIT 1005

U.S. Patent No. 7,036,143 to *Leung et al.*

("*Leung*")

US007036143B1

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

(10) **Patent No.: US 7,036,143 B1**
(45) **Date of Patent: Apr. 25, 2006**

(54) **METHODS AND APPARATUS FOR VIRTUAL PRIVATE NETWORK BASED MOBILITY**

(75) Inventors: **Keng Leung**, Mountain View, CA (US); **Alpesh S. Patel**, Santa Clara, CA (US)

(73) Assignee: **Cisco Technology, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 948 days.

(21) Appl. No.: **09/957,519**

(22) Filed: **Sep. 19, 2001**

(51) **Int. Cl.**
H04L 9/00 (2006.01)
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **726/15**; 713/168; 709/227; 726/5

(58) **Field of Classification Search** 713/150, 713/151, 168–170, 200–202; 709/227, 228, 709/230, 245
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,692,918	A	9/1987	Elliott et al.	370/85
5,016,244	A	5/1991	Massey et al.	370/16
5,018,133	A	5/1991	Tsukakoshi et al.	340/825.05
5,218,600	A	6/1993	Schenkyr et al.	370/16
5,371,852	A	12/1994	Attanasio et al.	395/200
5,473,599	A	12/1995	Li et al.	370/16
5,978,672	A	11/1999	Hartmaier et al.	455/413
6,016,428	A	1/2000	Diachina et al.	455/435.1
6,055,236	A	4/2000	Nessette et al.	370/389
6,075,783	A	6/2000	Voit	370/352
6,079,020	A *	6/2000	Liu	713/201
6,081,507	A	6/2000	Chao et al.	370/235
6,122,268	A	9/2000	Okanoue et al.	370/338
6,131,095	A	10/2000	Low et al.	707/10
6,137,791	A	10/2000	Frid et al.	370/352
6,144,671	A	11/2000	Perinpanathan et al.	370/409
6,154,839	A *	11/2000	Arrow et al.	713/154
6,173,399	B1 *	1/2001	Gilbrech	713/153
6,175,917	B1 *	1/2001	Arrow et al.	713/1
6,226,748	B1 *	5/2001	Bots et al.	713/201
6,226,751	B1 *	5/2001	Arrow et al.	713/201
6,339,830	B1	1/2002	See et al.	713/202
6,445,922	B1	9/2002	Hiller et al.	
6,522,880	B1	2/2003	Verma et al.	
6,683,871	B1	1/2004	Lee et al.	
6,701,437	B1 *	3/2004	Hoke et al.	713/201

OTHER PUBLICATIONS

S. Deering, Network Working Group Request For Comments 1256, "*ICMP Router Discovery Message*", Xerox PARC, Sep. 1991, pp. 1-19.

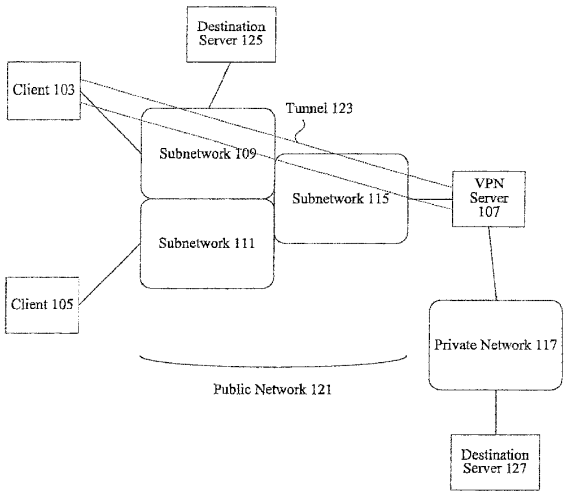
(Continued)

Primary Examiner—Christopher Revak
(74) *Attorney, Agent, or Firm*—Beyer Weaver & Thomas, LLP

(57) **ABSTRACT**

Methods and apparatus for enabling VPN based mobility are provided. A VPN client having a client subnetwork address corresponding to a particular subnetwork can create a VPN tunnel using an enterprise address from a VPN server. Using the VPN tunnel, the VPN client can establish sessions with a variety of destination nodes including destination nodes on a private or enterprise network associated with the VPN server. When the client moves, the VPN client can acquire a new address that may correspond to a new subnetwork, but the VPN server provides the VPN client with the same enterprise address. Accordingly, the VPN client can maintain existing sessions with destination nodes using the same enterprise address.

63 Claims, 10 Drawing Sheets



OTHER PUBLICATIONS

Gleeson et al., Network Working Group Request For Comments 2764, "*A Framework For IP Based Virtual Private Networks*", Lucent Technologies, Feb. 2000, Copyright © The Internet Society (2000). All rights reserved, pp. 1-62.

Tsirtsis et al., Network Working Group Request For Comments 2766, "*Network Address Translation—Protocol Translation (NAT-PT)*", Campio Communications, Feb. 2000, Copyright (C) The Internet Society (2000). All Rights Reserved, pp. 1-21.

E. Rosen et al., Network Working Group Request for Comments 2547, "*BGP/MPLS VPNs*", Cisco Systems, Inc., Mar. 1999, Copyright (C) The Internet Society (1999). All Rights Reserved., pp. 1-25.

Levkowetz, H. et al., "*Mobile IP NAT/NAPT Traversal using UDP Tunneling*", Internet Draft, Nov. 2001, 23 pages.

Khalil, Mohamed M. et al., "*Generalized NAI (GNAI) Extension for Mobile IPv4"*, Internet Draft, Oct. 2001, 6 pages.

Adrangi, Farid and Prakash, Iyer, "*Mobile IPv4 Traversal Across Firewalls*", Internet Draft, Nov. 13, 2001, 30 pages.

S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Nov. 1998, 50 pgs.

Steven Brown, "Implementing Virtual Private Networks".

Release notes for 3Com Corporation, "*Conducting a Redundant Route for Network Resiliency*," Mar. 1994, *NET Builder Family Bridge/Router* pp. 26-29.

Uyless Black, "*TCP/IP and Related Protocols*," 1992, *McGraw-Hill, Inc.*, pp. 226-249.

T. Li, et al., RFC 2281 "*Cisco Hot Standby Router Protocol (HSRP)*," Mar. 1998.

Chambless, et al., "*Home Agent Redundancy Protocol (HARP)*," Oct. 27, 1997.

C. Perkins, "*IP Mobility Support*," RFC 2002, IBM Corporation, Oct. 1996.

"*Mobil IP*," Release 12.0(1)T, pp. 1-55.

Montenegro, G., "*Reverse Tunneling for Mobile IP*," RFC 2344, Sun Microsystems, Inc., May 1998.

D. Harkins and D. Carrel, "*The Internet Key Exchange (IKE)*," Cisco Systems, Jun. 1998.

D. Cong and M. Hamlen, and C. Perkins, "*The Definitions of Managed Objects for IP Mobility Support using SMIv2*," RFC 2006, Motorola and IBM, Oct. 1996.

Aboba and Beadles, "*The Network Access Identifier*" RFC 2486, Jan. 1999.

Calhoun and Perkins, "*Mobile IP Network Access Identifier Extension, for IPv4*", Jan. 12, 2000.

Jonathan B. Postel, J., "*Simple Mail Transfer Protocol*", STD 10, RFC 821, Aug. 1982.

Crocker, D. and P. Overrell, "*Augmented BNF For Syntax Specifications: ABNF*", RFC 2234, Nov. 1997.

* cited by examiner

Figure 1

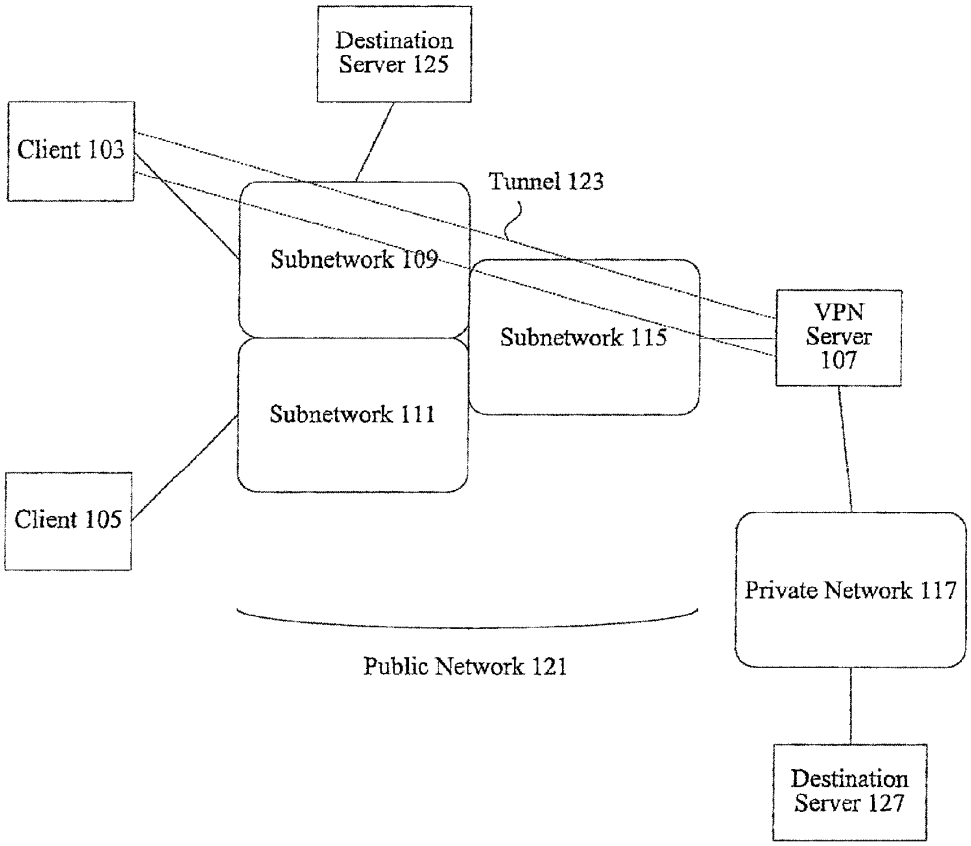

Destination Server 125
Client 103
Tunnel 123
Subnetwork 109
Subnetwork 115
VPN Server 107
Subnetwork 111
Client 105
Private Network 117
Public Network 121
Destination Server 127

Figure 2

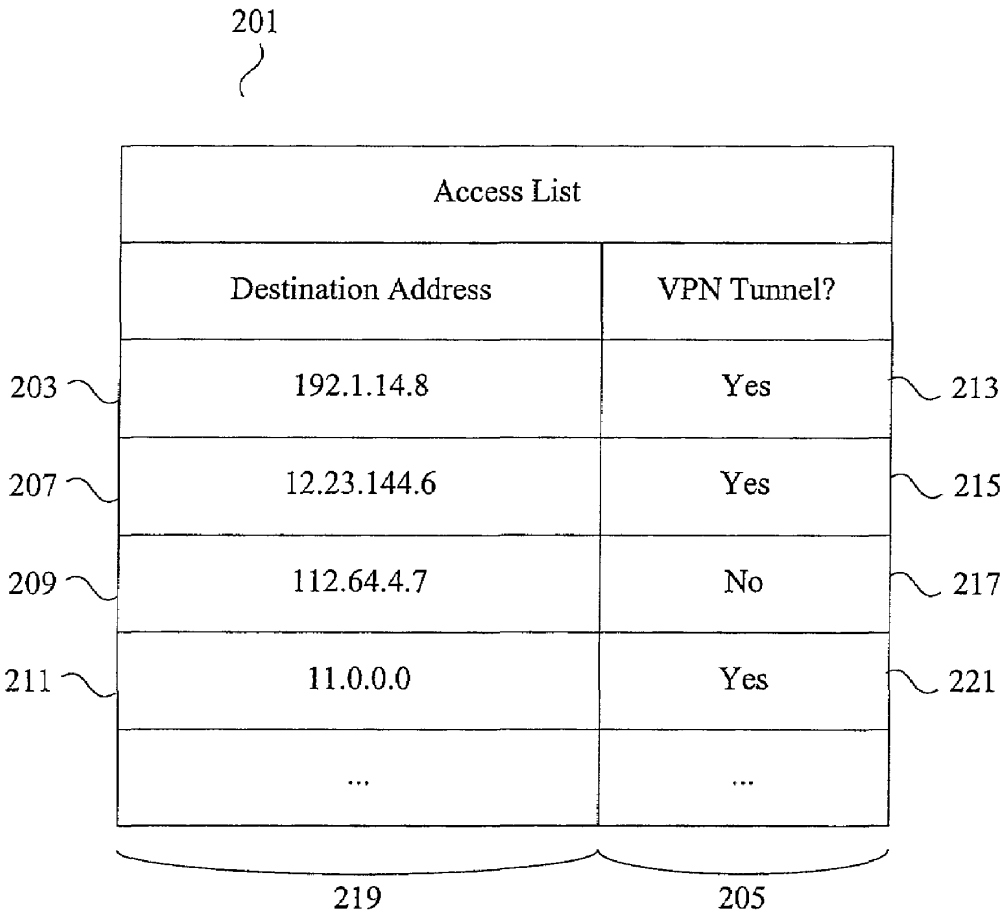

201
Access List
Destination Address
VPN Tunnel?
203
192.1.14.8
Yes
213
207
12.23.144.6
Yes
215
209
112.64.4.7
No
217
211
11.0.0.0
Yes
221
...
...
219
205

Figure 3

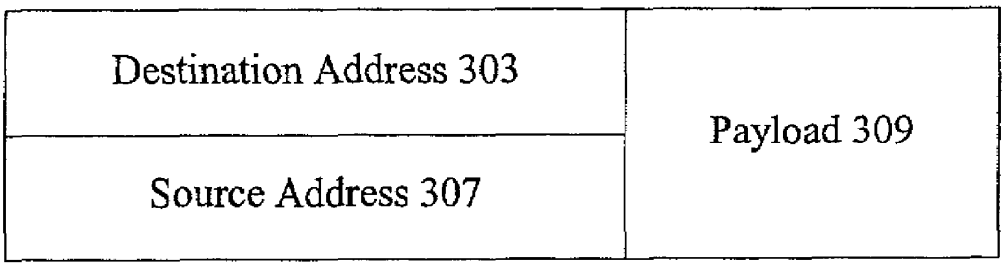


Figure 4A

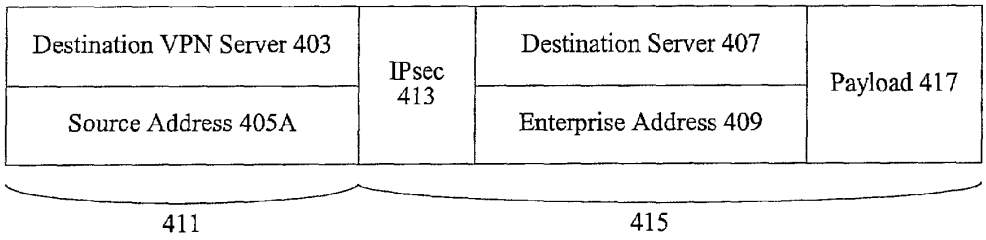


Figure 4B

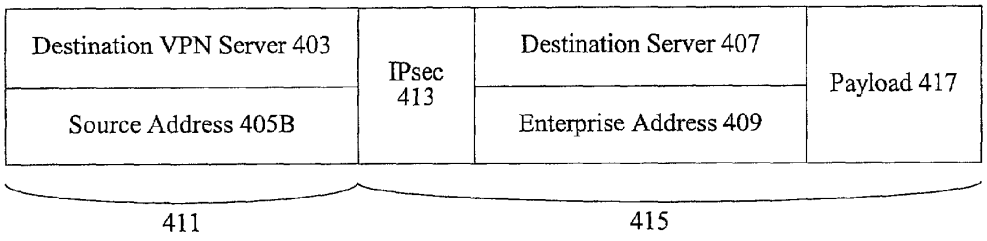


Figure 5

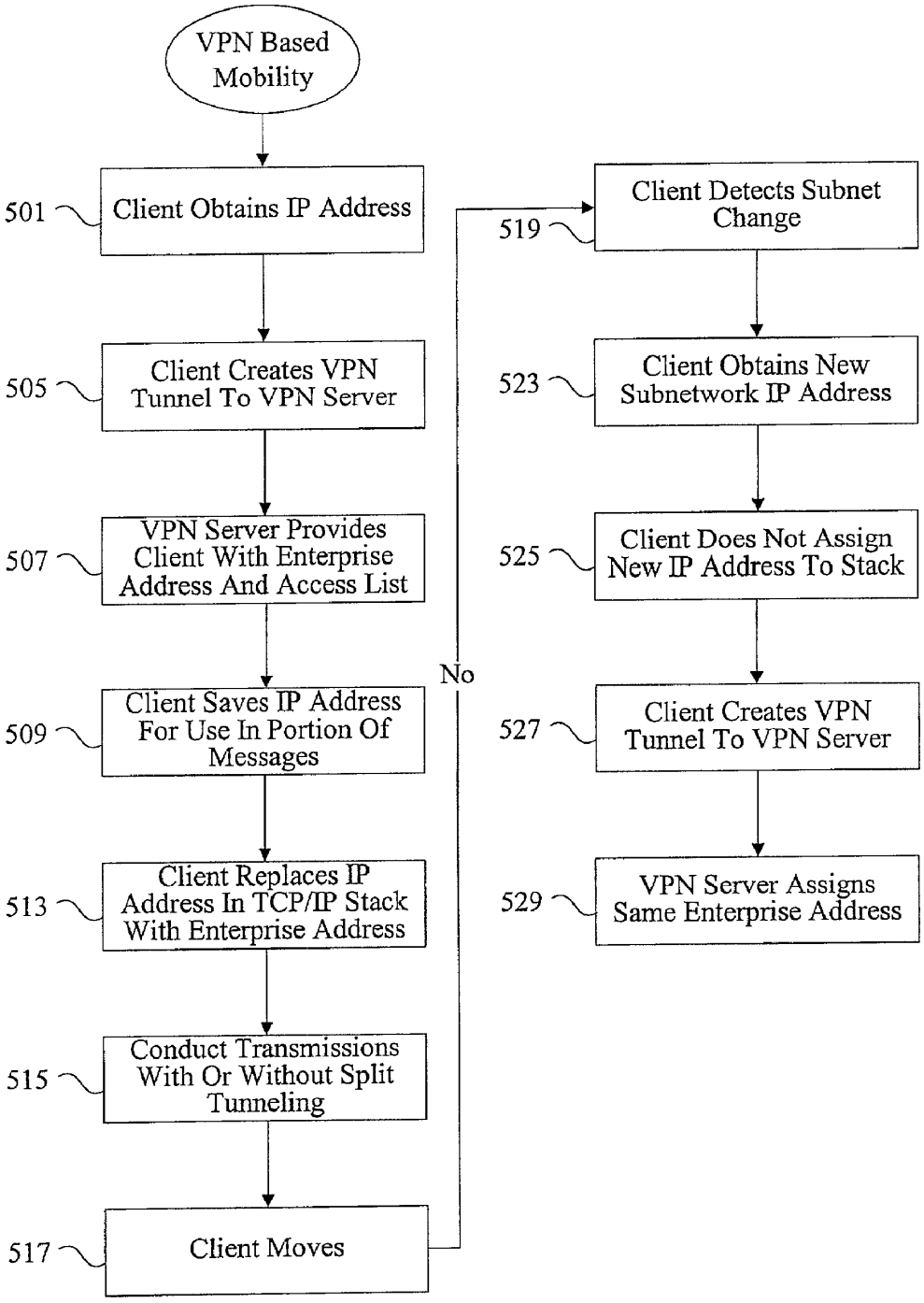
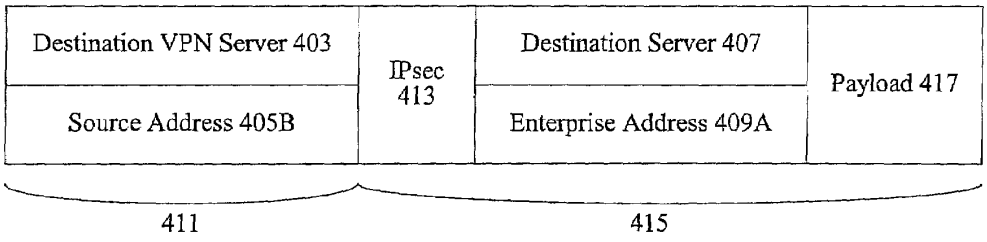
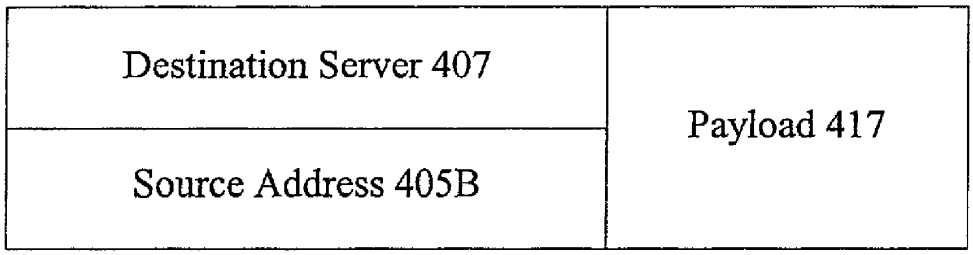

VPN Based Mobility
501
Client Obtains IP Address
505
Client Creates VPN Tunnel To VPN Server
507
VPN Server Provides Client With Enterprise Address And Access List
509
Client Saves IP Address For Use In Portion Of Messages
513
Client Replaces IP Address In TCP/IP Stack With Enterprise Address
515
Conduct Transmissions With Or Without Split Tunneling
517
Client Moves
No
519
Client Detects Subnet Change
523
Client Obtains New Subnetwork IP Address
525
Client Does Not Assign New IP Address To Stack
527
Client Creates VPN Tunnel To VPN Server
529
VPN Server Assigns Same Enterprise Address

Figure 6



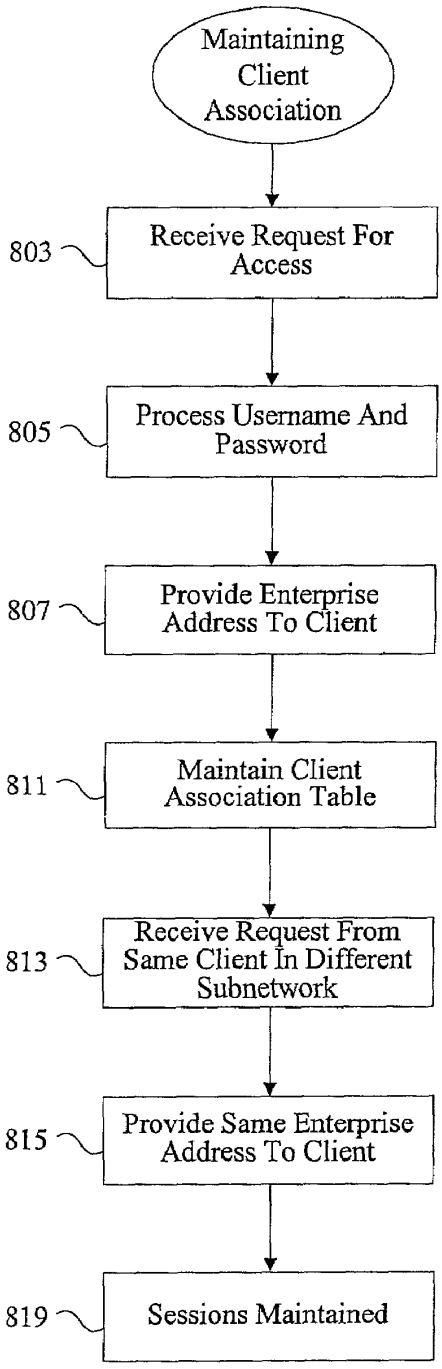
AA/SWA Ex. 1015, p.92 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Figure 7



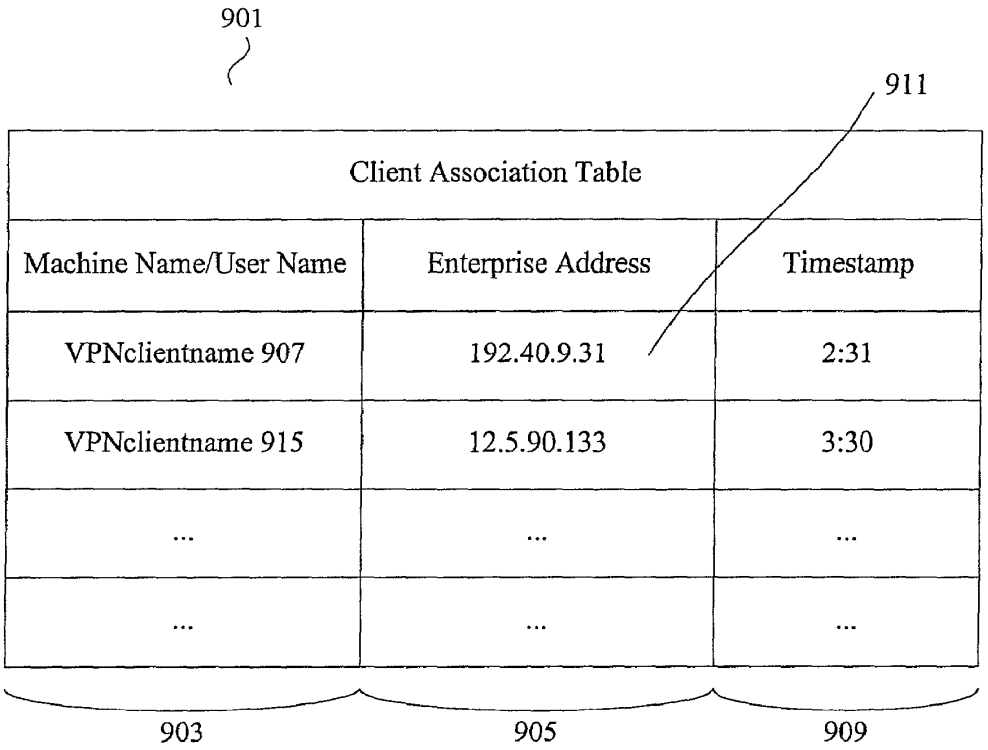
AA/SWA Ex. 1015, p.93 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Figure 8



AA/SWA Ex. 1015, p.94 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Figure 9


901
911
Client Association Table
Machine Name/User Name
Enterprise Address
Timestamp
VPNclientname 907
192.40.9.31
2:31
VPNclientname 915
12.5.90.133
3:30
...
...
...
...
...
...
903
905
909

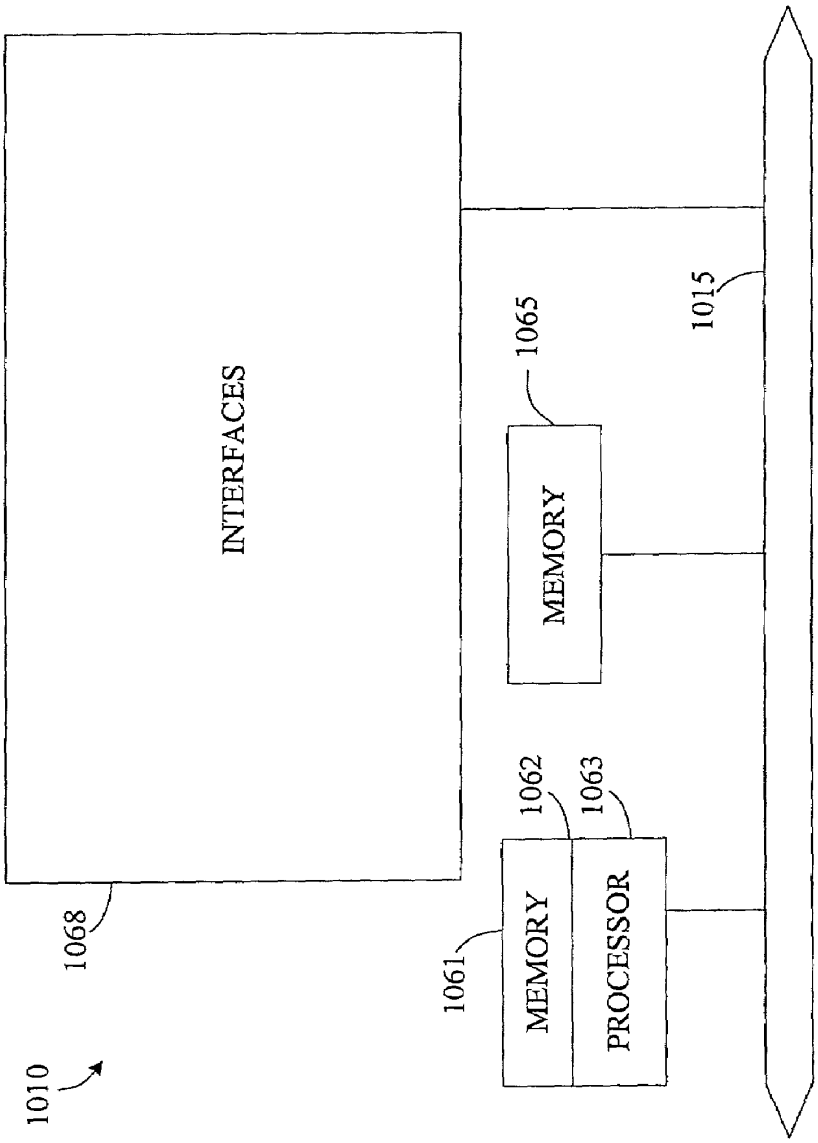

INTERFACES
1068
1010
1061
MEMORY
PROCESSOR
1062
1063
MEMORY
1065
1015

Figure 10

METHODS AND APPARATUS FOR VIRTUAL PRIVATE NETWORK BASED MOBILITY

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to virtual private networks. More particularly, the present invention relates to methods and apparatus enabling virtual private network based mobile communications.

2. Description of Related Art

Conventional virtual private networks deployed on a public network infrastructure provide clients the same security, management, quality of service policies, and benefits provided to clients in private networks. Typical applications of virtual private networks (VPN) allow remote network nodes such as telecommuters, suppliers, partners, or distant offices access to a private network such as a company network through a VPN server. Many VPN applications use IPsec (Internet Protocol Security) to provide encryption and authentication of messages between a VPN client and a VPN server. The secure connection between a VPN client and a VPN server is often referred to as a VPN tunnel. In most cases, a VPN client accessing a private network through a VPN tunnel can enjoy the same privileges and access capabilities as a client within the private network.

However, conventional virtual private networks have not been designed to allow mobile VPN clients. A VPN client with a particular client IP subnetwork address associated with a particular subnetwork can typically only access the private network through the VPN server as long as the VPN client maintains the same IP subnetwork address. If the IP subnetwork address of the VPN client changes, the sessions the VPN client has with the nodes in the private network are terminated. It should be noted that a client is generally referred to as a VPN client after a VPN tunnel is established. However, a potential VPN client with a VPN tunnel either broken or not established will still be referred to herein as a VPN client for clarity.

More particularly, the IP subnetwork address of the VPN client changes when the VPN client moves from a first subnetwork to a second subnetwork. For example, a laptop user riding on a train may be accessing a private network through a VPN server. The laptop user may be assigned a particular IP subnetwork address associated with a first subnetwork. However, when the vehicle moves into a second subnetwork, a new IP subnetwork address is assigned to the laptop user. The VPN tunnel is not maintained when the IP subnetwork address of the VPN client changes. Thus, after moving to a different subnetwork, the VPN client can only access the private network by establishing a new VPN tunnel to the VPN server. However, establishing a new VPN tunnel disrupts any sessions that the VPN client may have been conducting with network nodes. As a result, this disruption prevents seamless communications between the VPN client and various network nodes when the client moves. Virtual Private Networks are described in more detail in *Implementing Virtual Private Networks* by Steven Brown (ISBN: 007135185X), the entirety of which is incorporated by reference for all purposes.

Other standards such as MobileIP allow users to maintain existing sessions when moving between various subnetworks. However, many conventional MobileIP standards do not provide for secure connections. Furthermore, not all clients wishing to access a home network securely have Mobile IP. Consequently, it is desirable to provide improved mobility solutions for VPN clients using VPN.

SUMMARY OF THE INVENTION

Methods and apparatus for enabling VPN based mobility are provided. A VPN client having a client subnetwork address corresponding to a particular subnetwork can create a VPN tunnel and obtain an enterprise address from a VPN server. Using the VPN tunnel, the VPN client can establish sessions with a variety of destination nodes including destination nodes on a private or enterprise network associated with the VPN server. When the client moves, the VPN client can acquire a new address that may correspond to a new subnetwork, but the VPN server provides the VPN client with the same enterprise address. Accordingly, the VPN client can maintain existing sessions with destination nodes using the same enterprise address.

When a client moves from one subnetwork to a new subnetwork, the client can maintain its enterprise address knowing that the VPN server can assign it the same enterprise address. By reusing the same enterprise address, client sessions are not terminated.

In one embodiment, a method for allowing VPN based mobile communications in a network having a VPN server and a VPN client is provided. A first message is received from the VPN client, the first message having a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address. An association between the enterprise address and the VPN client is maintained. A second message from the VPN client is received, the second message having a second address associated with a second subnetwork as the source address and the enterprise address as the encapsulated address, wherein using the same enterprise address allows VPN based mobile communications when a VPN client moves from the first subnetwork to the second subnetwork.

In another embodiment, an apparatus for allowing VPN based mobile communications in a network having a VPN server and a VPN client is provided. The apparatus includes means for receiving a first message from the VPN client, the first message having a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address, means for maintaining an association between the enterprise address and the VPN client, and means for receiving a second message from the VPN client, the second message having a second address associated with a second subnetwork as the source address and the enterprise address as the encapsulated address, wherein using the same enterprise address allows VPN based mobile communications when a VPN client moves from the first subnetwork to the second subnetwork.

In yet another embodiment, a method for allowing communication in a network having a VPN server and a VPN client is provided. The method includes transmitting a first message to the VPN server with a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address, detecting a change in location of the VPN client from the first subnetwork to a second subnetwork, and transmitting a second message to the VPN server with a second address associated with the second subnetwork as the source address and the enterprise address as the encapsulated address, wherein encapsulating the same enterprise address allows communication when a VPN client moves from a first subnetwork to a second subnetwork.

In another embodiment, an apparatus for allowing communication in a network having a VPN server and a VPN client is provided. The apparatus includes memory and a processor coupled to memory, the processor configured to

AA/SWA Ex. 1015, p.97 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

transmit a first message to the VPN server with a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address, detect a change in location of the VPN client from the first subnetwork to a second subnetwork and transmit a second message to the VPN server with a second address associated with the second subnetwork as the source address and the enterprise address as the encapsulated address, wherein encapsulating the same enterprise address allows communication when a VPN client moves from a first subnetwork to a second subnetwork.

Another aspect of the invention pertains to computer program products including a machine readable medium on which is stored program instructions, tables or lists, and/or data structures for implementing a method as described above. Any of the methods, tables, or data structures of this invention may be represented as program instructions that can be provided on such computer readable media.

A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may best be understood by reference to the following description taken in conjunction with the accompanying drawings, which illustrate specific embodiments of the present invention.

FIG. **1** is a diagrammatic representation of a system that can use the techniques of the present invention.

FIG. **2** is a diagrammatic representation of an access list that a VPN server may transmit to a VPN client.

FIG. **3** is a diagrammatic representation of a message a VPN client can transmit using split tunneling.

FIG. **4**A is a diagrammatic representation of a message a VPN client can transmit using a VPN tunnel.

FIG. **4**B is a diagrammatic representation of a message a VPN client can transmit using a VPN tunnel when the VPN client moves to a different subnetwork.

FIG. **5** is a process flow diagram showing VPN client processes that can allow mobility.

FIG. **6** is a diagrammatic representation of a message a VPN client in a second subnetwork can transmit.

FIG. **7** is a diagrammatic representation of a message a VPN client in a second subnetwork can transmit using split tunneling.

FIG. **8** is a process flow diagram showing VPN server processes that can allow mobility.

FIG. **9** is a diagrammatic representation of a client association table.

FIG. **10** is a diagrammatic representation of a system that can be used to implement a VPN client or VPN server.

DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be obvious, however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In other instances, well known process steps have not been described in detail in order not to unnecessarily obscure the present invention.

Conventional virtual private networks do not allow VPN clients to move between subnetworks without breaking existing sessions. More particularly, a VPN client in a particular subnetwork can acquire a client subnetwork address from an Internet Service Provider (ISP). The client subnetwork address, however, is typically specific to the particular subnetwork that is servicing the client at that particular time. The client may therefore use the client subnetwork address to contact the VPN server and provide the VPN server with a user name and password to acquire an enterprise address. The enterprise address is the address that the VPN client uses to communicate with other nodes such as nodes in the company private network. A client that at some point sets up a session with a VPN server is referred to herein as a VPN client. For instance, the enterprise address can be a company IP address. Thus, other nodes including nodes in the company private network will see the VPN client as having the enterprise address, and will therefore communicate with the VPN client via the enterprise address. Accordingly, sessions between the VPN client and a node of the private network can be conducted using the enterprise address. It should be noted that a client can have two distinct addresses. An address specific to a particular subnetwork that can be obtained from an ISP is referred to herein as a subnetwork address or a client subnetwork address. The subnetwork address can be an IP address. An address provided by a VPN server and assigned to the client is referred to herein as an enterprise address.

Traditionally, by using the subnetwork address and the enterprise address, the VPN client can maintain a VPN tunnel between itself and the VPN server. However, when the subnetwork address of the VPN client changes, the VPN tunnel is broken. In conventional systems, the VPN client is typically required to contact the VPN server with a new subnetwork address, a user name, and password to acquire a new enterprise address. The new enterprise address allows the creation of a new VPN tunnel, but existing sessions are dropped. Thus, restarting a VPN tunnel can be disruptive.

The present invention provides methods and apparatus for improving client mobility. In one embodiment, the VPN client is modified to use the same enterprise address whether it is accessing the VPN server from a first subnetwork or from a second subnetwork. The VPN server can be modified to maintain an association between the VPN client and the enterprise address. By using the same enterprise address, existing sessions between the VPN client and various nodes such as nodes in a private network can be maintained. Even when a VPN client moves from a first subnetwork to a second subnetwork, other nodes see the VPN client as maintaining a single enterprise address. Thus, other nodes, including nodes in the company private network, will see that the VPN client still has the same enterprise address and will be able to maintain existing sessions.

It should be noted that although the techniques of the present invention will be described in the context of IPsec based VPN, variations to VPN are contemplated. For example, encryption protocols such as DES and Triple DES can be used in IPsec. VPN as well as VPN variants are referred to herein as VPN.

FIG. **1** is a diagrammatic representation of a system in which embodiments of the present invention may be implemented. The subnetworks **109**, **111**, and **115** are part of a public network **121**. The public network **121** can be connected with a variety of private networks as well as other public networks through different network nodes. For example, the public network **121** is connected to private network **117** through a VPN server **107**. As shown, a destination server **127** may be part of the private network **117**. The public network **121** is also connected to a destination server **125** as well as clients **103** and **105**. In one

example, a client **103** may be a laptop attempting to access a company private network **117** through public network **121** and VPN server **107**. For instance, client **103** may be connected to public network **121** through an Internet service provider. In this example, client **103** may acquire a subnetwork address from the Internet service provider associated with subnetwork **109**.

When the subnetwork address is obtained, the subnetwork address may be specifically associated with subnetwork **109**. Using the subnetwork address, client **103** can access a destination server **125** in a public network **121**. However, client **103** can not access a private network destination server **127** until it is granted access by VPN server **107**. To acquire access to destination server **127** in a private network **117**, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server **107**. In the access request, the client **103** provides information such as its subnetwork address, its user name, and its password. The VPN server **107** verifies the user name and password information from client **103** and provides the client **103** with an enterprise address. The enterprise address can be any address that allows a VPN server to identify a client **103**. According to various embodiments, the enterprise address is a subnetwork address associated with the private network **117**. For instance, the enterprise address may be a company IP address. VPN server **107** and client **103** also exchange messages to allow encryption and authentication of messages transmitted between the two network nodes. As will be appreciated by one of skill in the art, encryption and authentication can be accomplished using IPsec.

The use of encryption, authentication, and the enterprise address allow a VPN tunnel **123** to be established between client **103** and VPN server **107**. It should be noted that VPN tunnel **123** is an abstraction depicting the secure traffic flow between client **103** and VPN server **107**. VPN tunnels will be described in further detail below. Even though the abstraction provides for a VPN tunnel between client **103** and VPN server **107**, messages flowing between client **103** and VPN server **107** may actually flow through a variety of additional network nodes in a public network **121**. A VPN server **107** not only provides client **103** with information to create a VPN tunnel **123**, the VPN server **107** also provides client **103** with an access list. In typical implementations, the access list provides information to a client **103** regarding which messages should be sent through a particular VPN tunnel, as will be described in further detail below.

As will be appreciated by one of skill in the art, an access list can be used to allow split tunneling. Split tunneling provides that messages associated with particular destinations are sent directly to the destination while other messages are sent to various destinations through a VPN tunnel **123** and VPN server **107**. According to various embodiments, nodes on a private network **117** are accessed through VPN tunnel **123** while nodes on public network **121** are accessed directly. According to other embodiments, both nodes on a private network **117** and nodes on a public network **121** are accessed through VPN tunnel **123**.

FIG. **2** is a diagrammatic representation of an access list that a VPN server **107** may send to client **103** to provide information for split tunneling. Access list **201** contains a column **219** of destination addresses and a column **205** indicating whether or not to use a VPN tunnel. Each destination address **203**, **207**, and **209** may be a subnetwork address. A flag **213**, **215**, or **217** is used to indicate whether messages destined for a corresponding address **203**, **207**, or **209** should be sent via a VPN tunnel, and therefore should be encrypted. In one example, a client **103** may wish to transmit a message to destination address **203** corresponding to 192.1.14.8. A client **103** can perform a lookup to see whether messages sent to destination address **203** should be sent through a VPN tunnel. Upon determining that the message should be encrypted, the client can send any message to destination address **203** through VPN tunnel **213**. As will be appreciated by one of skill in the art, an access list may not always be used in various implementations of VPN.

The access lists may also be represented in a variety of manners. In one embodiment, only destination addresses that should be accessed through a VPN tunnel are listed in the access list. In another embodiment, only destination addresses that should be accessed directly are listed. Any access list indicator including flags can be used to indicate that a particular message should be sent through a VPN tunnel to a VPN server. The VPN server can then direct messages out to the appropriate destination.

According to various embodiments, split tunneling is not used. When split tunneling is not used, all messages sent from a client are sent to the VPN server through a VPN tunnel without regard to an access list.

FIG. **3** is a diagrammatic representation of a message that can be sent out directly out to the network without the use of a VPN tunnel. The source address **307** can be the subnetwork address of the client transmitting the message. The destination address **303** can be the subnetwork address of the content server or destination server that the client is attempting to access. The payload **309** may contain information or a request for information. As will be appreciated by one of skill in the art, messages may contain other information such as the length of a packet, number of hops, quality of service information, etc. The source address **307** and the destination address **303** can be used for communications between the client node and the destination node without the use of a VPN tunnel.

In accordance with various embodiments, a VPN tunnel should be established to send a message from a client outside the private network to a node within the private network, or from a node within the private network to a client outside the private network. FIG. **4**A is a diagrammatic representation of a message that can be sent from a client to a destination when a VPN tunnel is used. For example, the source address **405**A can be the subnetwork address of the client. Moreover, in this example, the destination address is the subnetwork address of the VPN server **403**. In one embodiment, in order for a VPN client to send a message to a VPN server, the VPN server address **403** and the subnetwork address **405** are contained in the outer portion **411** of the message. The outer portion of **411** is typically not encrypted to allow the message **401** to be routed using conventional routing mechanisms to a VPN server.

In this example, the encapsulated portion **415**, however, is typically encrypted using IPsec **413**. Encapsulated portion **415** provides the VPN tunnel with security. More particularly, security is provided through enabling authentication of the sender (e.g., via information in the encapsulated portion **415**) and encryption of data as well. For instance, the encapsulated portion **415** preferably contains the enterprise address **409** allocated by the VPN server to the VPN client during the creation of the VPN tunnel, which may be used to authenticate the sender. The encapsulated portion **415** also contains the destination address of the server **407** that the client wishes to access. In one example, the destination server **407** may be a Web server containing a page that the client wishes to view. The encapsulated portion **415** may also contain a payload **417**.

In one implementation, a client wishes to access a Web server. A client examines the access list to determine if the Web server address is on the access list. If the Web server address is not on the access list, the client can send a packet directly to the Web server using its subnetwork address as the source address and the address of the Web server as the destination address, as shown above. If the Web server is on the access list, the client is directed to send a packet to the Web server through a VPN tunnel and a VPN server. The client uses its own address as the source address and the address of the VPN server as the destination address of a message. The message contains an encapsulated portion **415** with a destination address **407** set as the address of the Web server and the source address **409** set as the enterprise address allocated by the VPN server. When the VPN server receives the message, the VPN server can decrypt the message, authenticate the sender via the enterprise address (source address **409**) and forward the encapsulated portion **415** of the message to the Web server.

The Web server receives the encapsulated portion of the message and sees that the source of the message is the enterprise address. The Web server can send content to the enterprise address represented by the VPN server. The VPN server can then encapsulate the content and forward the content to the client. As noted above, the Web server does not know the actual subnetwork address of the client. The Web server may only know the enterprise address. In other words, the VPN server performs a mapping of the enterprise address to the client address.

When a client moves from one subnetwork to another subnetwork, the client typically acquires a new subnetwork address associated with the new subnetwork. In one example, a client can be a personal digital assistant user accessing a corporate network. More particularly, the client may be riding in a vehicle moving from one subnetwork to another subnetwork. When a client moves from a first subnetwork to a second subnetwork, the client typically acquires a new subnetwork address associated with the second subnetwork. When the client acquires the new subnetwork address associated with the second subnetwork, the VPN tunnel is broken. Conventional VPN servers do not accept packets from the same client having different (e.g., unrecognizable) source addresses.

When the VPN tunnel is broken, the client typically tries to reinitiate the VPN tunnel. The client sends the VPN server its new subnetwork address, a user name, and a password, and the VPN server provides the client with a new enterprise address. FIG. **4**B is a diagrammatic representation of a message that a client in a new subnetwork can transmit to a VPN server. The source address **405**B is the new subnetwork address associated with the new subnetwork. The destination address is the VPN server address **403**. It should be noted that the destination address is still the same VPN server address as it was when the client was still in the first subnetwork. The encapsulated portion of the message contains the address of a destination server **407** such as a Web server and the new enterprise address **409** allocated during creation of the VPN tunnel when the client moved to the new subnetwork. Sessions that the client may have had when a client was in a first subnetwork are not maintained when the client moves into the second subnetwork. One reason is that the enterprise address is no longer the same. In other words, the enterprise address previously assigned to the client no longer exists. Thus, the movement of a client from a first subnetwork to a second subnetwork causes the disruptive dropping of sessions.

The present invention allows the maintenance of existing sessions between a client and a destination node when the client moves from a first subnetwork to a second subnetwork. According to various embodiments, existing sessions can be maintained by modifying the VPN client and the VPN server. More particularly, the VPN client and the VPN server can be modified to allow the VPN client to use the same enterprise address whether the VPN client is in a first subnetwork or a second subnetwork. By using the same enterprise address, a client's existing sessions with a Web server, for example, can be maintained because the Web server can continue to send messages to the client using the same address.

FIG. **5** is a process flow diagram depicting some of the changes that can be made to the VPN client to allow the VPN client to seamlessly roam from a first subnetwork to a second subnetwork. At **501**, a client is in a first subnetwork and obtains a first subnetwork address from an Internet service provider. The first subnetwork address is inserted into the TCP/IP stack to allow communication with other nodes in the network. At **505**, the client attempts to set up a VPN tunnel with the VPN server by transmitting the first subnetwork address, a username, and a password to the VPN server. The VPN server verifies the information and provides the client with an enterprise address as well as an access list at **507**. At **509**, the client saves the first subnetwork address to use as an outer portion source address for outgoing packets. For instance, the first subnetwork address can be saved in the device driver or in the operating system. At **513**, the VPN client replaces the first subnetwork address in the TCP/IP stack with the enterprise address acquired from the VPN server. By replacing the first subnetwork address with the enterprise address, the enterprise address can be used for all communications whether the client is in a first subnetwork or a second subnetwork. At **515**, the client can send messages with or without the VPN tunnel. If messages are sent without the VPN tunnel, the source address is the first subnetwork address and the destination address can be the destination node of interest. If messages are sent through the VPN tunnel, the source address is the first subnetwork address and the destination address is the address of the VPN server. The encapsulated destination address is the destination node of interest and the encapsulated source address is the enterprise address. Such a message resembles the message shown in FIG. **4**A.

At **517**, the client moves from a first subnetwork to a second subnetwork. At **519**, the client detects the change in subnetworks without user intervention. One of the benefits of the techniques of the present invention is that VPN based mobility can be accomplished in a manner transparent to the user. In many conventional applications, the client moving from a first subnetwork to a second subnetwork had to acquire a new subnetwork address and manually start the creation of a new VPN tunnel. Existing sessions would be dropped. However, the techniques of the present invention allow a VPN tunnel and existing sessions to be maintained without user interaction. The seamless mobility can be accomplished by automatically detecting a change in subnetwork using lower layer protocols. A variety of conventional mechanisms for detecting subnet changes are available. Some techniques include using the lifetime field from a router advertisement using IRDP as described in RFC 1256 or using network prefixes as described in RFC 2002, the entirety of which is incorporated by references for all purposes.

The VPN client can then automatically obtain a second subnetwork address associated with the second subnetwork

UNIFIED PATENTS EXHIBIT 1005
Page 16 of 20

AA/SWA Ex. 1015, p.100 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

at **523**. In one embodiment, the second subnetwork address can be obtained using DHCP. In other embodiments, a second subnetwork address can be automatically entered by a VPN client. At **525**, the VPN client recognizes the change in subnetworks and does not replace the enterprise address in the TCP/IP stack with the second subnetwork address. The second subnetwork address instead can be saved in the device driver. The enterprise address remains the same in the TCP/IP stack. Without user intervention, the VPN client automatically attempts to re-establish the VPN tunnel by sending the second subnetwork address, a username, and a password to the VPN server. The tunnel to the VPN server is created at **527**. Because of modifications to the VPN server which will be discussed below, the VPN server assigns the same enterprise address to the VPN client at **529**. By providing the same enterprise address to the VPN client, existing sessions are maintained. As will be appreciated by one of skill in the art, although the techniques of the present invention can be accomplished without user intervention, it will be appreciated that certain circumstances may benefit from user input. Various techniques for acquiring a new subnetwork address and establishing a VPN tunnel can also be accomplished manually.

FIG. **6** is a diagrammatic representation of a packet that the VPN client may send to the VPN server after the VPN server has assigned the same enterprise address to a VPN client that has moved to the second subnetwork. Outer portion **411** contains a destination address set as the address of the destination VPN server **403**. The source address is set as the second subnetwork address **405**B associated with a second subnetwork. The encapsulated portion **415** contains the destination address **407** of a server such as a Web server. The encapsulated portion **415** also contains the same enterprise address **409** that was used when a VPN client was in a first subnetwork. As noted above, using the same enterprise address **409** allows existing sessions to be maintained.

The VPN client can also send messages out directly onto a network without the use of a VPN tunnel. The VPN client may send a message directly out onto the network when the access list indicates that the destination may be reached without using a VPN tunnel. The techniques of the present invention allow for split tunneling. FIG. **7** is a diagrammatic representation of a packet that the VPN client may send directly to a destination without the use of a VPN tunnel. As shown, the destination address **407** can be the address of the content server of interest, while the source address **405**B can be the second subnetwork address associated with the second subnetwork.

As noted above, modifications to a VPN server are made to allow the allocation of the same enterprise address to a mobile VPN client regardless of whether the client is in a first subnetwork or a second subnetwork. FIG. **8** is a process flow diagram showing modifications to the server that can be used to provide a VPN client with the same enterprise address. At **803**, the VPN server receives a request for access. The request for access may include the subnetwork address, a username, and a password of a VPN client. At **805**, the VPN server verifies the username and password. At **807**, the VPN server provides an enterprise address to the VPN client to allow the VPN client to establish a VPN tunnel.

The VPN server maintains a client association table at **811**. Any mechanism providing an association between the client and the enterprise address is referred to herein as a client association table. For instance, the client association table can be maintained in a table listing usernames and their associated enterprise addresses. The client association table can also be maintained using various databases and log files providing information on client identifiers, usernames, and enterprise addresses. By maintaining an association between the client and the enterprise address, the VPN server can provide the same enterprise address to a client even if the client is registering from a different subnetwork address associated with a different subnetwork. If a client moves from a first subnetwork to a second subnetwork and registers with a second subnetwork address, the VPN server can recognize the client with the username. At **813**, the VPN server receives an access request having a second subnetwork address, a username, and a password of the same VPN client. The VPN server can access the client association table to determine whether the VPN client has been provided an enterprise address in the past. The VPN server can then provide the VPN client the same enterprise address.

By maintaining the association between the client and the enterprise address, the enterprise address can be provided to the same client at **815** even though the client is registering with a different subnetwork address. By maintaining the enterprise address, sessions are maintained at **819**.

FIG. **9** is a diagrammatic representation of an exemplary client association table that can be used in accordance with various embodiments of the invention. As shown, column **903** is a list of machine names/usernames that are stored in the client association table **901**. Column **905** is a list of enterprise addresses associated with the usernames. In one example, VPNclientname **907** may include information on both a machine name and a user name to conduct video and audio sessions with nodes in a private network. In this manner, the client association table allows an association of usernames with enterprise addresses.

Column **909** can contain timestamps providing information on how long the entry should be maintained. According to various embodiments, entries in the client association table can be maintained for any period of time. The length of time the entry is maintained can be determined by considering the number of enterprise addresses available to the VPN server and the typical amount of time the VPN client takes to reinitiate a VPN tunnel upon moving to a second subnetwork. In one example, if the VPN server has abundant enterprise addresses, each VPN client can be permanently associated with an enterprise address. Of course, if the VPN server has few enterprise addresses, the association between the VPN client and the enterprise address may be brief to allow other VPN clients access to a private network. Similarly, if the time it takes for a VPN client to register in any new subnetwork is brief, the entry in the client association table can be maintained for a brief period of time. If, however, a VPN client takes a substantial amount of time to register in a new subnetwork, the entry in a client association table can be maintained for a longer period of time. According to various embodiments, the entry in the client association table is maintained for 15 minutes, although the range can vary from seconds to days.

Although the techniques of the present invention have been discussed with reference to VPN, one of skill in the art will appreciate that the techniques can be used with a variety of different architectures including variants to VPN. Moreover, different encryption algorithms can also be used to provide security for the VPN tunnel.

Generally, the VPN mobility techniques may be implemented on software and/or hardware. For example, each of the described techniques can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, in a device driver on a specially constructed machine, or on a network inter-

face card. According to specific embodiments, the techniques of the present invention are implemented in software such as an operating system or in an application running on an operating system.

Software or software/hardware hybrid implementations of the invention may be implemented on general-purpose programmable machines selectively activated or reconfigured by a computer program(s) stored in memory. Such programmable machines may be a network device designed to handle network traffic. Such network devices typically have multiple network interfaces including frame relay and ISDN interfaces, for example. The present invention may be implemented on a general-purpose network host machine such as a personal computer or workstation. Further, the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general-purpose computing device.

A VPN client or a VPN server can be implemented on a general purpose computing device. FIG. **10** is a diagrammatic representation of a general purpose computing device that can be used. The computing system **1010** suitable for implementing the present invention includes a master central processing unit (CPU) **1062**, interfaces **1068**, and a bus **1015** (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU **1062** is responsible for tasks such as acquiring a subnetwork address or assigning an address to a TCP/IP stack. On the VPN server side, the CPU **1062** may be responsible for maintaining associations between clients and enterprises. The CPU **1062** may be a general purpose processor or it may be specially designed hardware for implementing a VPN client or a VPN server. In a specific embodiment, a memory **1061** (such as non-volatile RAM and/or ROM) also forms part of CPU **1062**. However, there are many different ways in which memory could be coupled to the system. Memory hlock **1061** may he used for a variety of purposes such as, for example, caching and/or storing data, programming instructions, etc.

The interfaces **1068** are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receiving of data packets over the network and sometimes support other peripherals used with the router **1010**. Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided such as fast Ethernet interfaces, Gigabit Ethernet interfaces, ATM interfaces, HSSI interfaces, POS interfaces, FDDI interfaces and the like. Generally, these interfaces may include ports appropriate for communication with the appropriate media. In some cases, they may also include an independent processor and, in some instances, volatile RAM. The independent processors may control such communications intensive tasks as packet switching, media control and management. By providing separate processors for the communications intensive tasks, these interfaces allow the master microprocessor **1062** to efficiently perform routing computations, network diagnostics, security functions, etc.

Although the system shown in FIG. **10** is one specific network node of the present invention, it is by no means the only VPN client or VPN server on which the present invention can be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc. is often used. Further, other types of interfaces and media could also be used with the router.

Regardless of network device's configuration, it may employ one or more memories or memory modules (such as, for example, memory block **1065**) configured to store data, program instructions for the general-purpose network operations and/or the packet redirection and replication functions described herein. The program instructions may control the operation of an operating system and/or one or more applications, for example. The memory or memories may also be configured to store the client association table or the access lists noted above.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as optical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). The invention may also be embodied in a carrier wave travelling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

While the invention has been particularly shown and described with reference to specific embodiments thereof, it will be understood by those skilled in the art that changes in the form and details of the disclosed embodiments may be made without departing from the spirit or scope of the invention. For example, the embodiments described above may be implemented using firmware, software, or hardware. Moreover, embodiments of the present invention may be employed with a variety of communication protocols and should not be restricted to the ones mentioned above. For example, the VPN server may be connected to multiple private networks only one of which the VPN client has access to. The public network may also include a variety of disparate networks such as LANs, WANs, wireless networks, etc. Therefore, the scope of the invention should be determined with reference to the appended claims.

The invention claimed is:

1. A method for allowing VPN based mobile communications in a network having a VPN server and a VPN client, the method comprising:

receiving a first message from the VPN client, the first message having a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address;

maintain an association between the enterprise address and the VPN client;

receiving a second message from the VPN client, the second message having a second address associated with a second subnetwork as the source address and the enterprise address as the encapsulated address, wherein using the some enterprise address allows VPN based mobile communications when a VPN client moves from the first subnetwork to the second subnetwork.

2. The method of claim **1**, further comprising providing the VPN client with an access list identifying one or more destinations that can be accessed through the VPN server.

3. The method of claim **1**, wherein the first and second messages are associated with an established VPN tunnel.

4. The method of claim 1, wherein the encapsulated address but not the source address is encrypted.

5. The method of claim 1, wherein the enterprise address is a private network IP address.

6. The method of claim 1, wherein using the same enterprise address allows VPN based mobile communications to continue seamlessly.

7. The method of claim 1, wherein maintaining an association between the enterprise address and the VPN client comprises associating the enterprise address with a username.

8. The method of claim 7, wherein the enterprise address is further associated with a password.

9. The method of claim 1, further comprising:

providing the enterprise address associated with the user to the VPN client.

10. The method of claim 9, further comprising:

authenticating the VPN client prior to providing the enterprise address associated with the VPN client to the VPN client.

11. The method of claim 9, wherein the enterprise address is provided by accessing the client association table.

12. An apparatus for allowing VPN based mobile communications in a network having a VPN server and a VPN client, the apparatus comprising:

means for receiving a first message from the VPN client, the first message having a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address;

means for maintaining an association between the enterprise address and the VPN client;

means for receiving a second message from the VPN client, the second message having a second address associated with a second subnetwork as the source address and the enterprise address as the encapsulated address, wherein using the same enterprise address allows VPN based mobile communications when a VPN client moves from the first subnetwork to the second subnetwork.

13. The apparatus of claim 12, further comprising providing the VPN client with an access list identifying one or more destinations that can be accessed through the VPN serer.

14. The apparatus of claim 12, wherein the first and second messages are associated with an established VPN tunnel.

15. The apparatus of claim 12, wherein the encapsulated address but not the source address is encrypted.

16. The apparatus of claim 12, wherein the enterprise address is a private network IP address.

17. The apparatus of claim 12, wherein using the same enterprise address allows VPN based mobile communications to continue seamlessly.

18. The apparatus of claim 12, wherein main an association between the enterprise address and the VPN client comprises associating the enterprise address with a username.

19. The apparatus of claim 18, wherein the enterprise address is further associated with a password.

20. The apparatus of claim 12, further comprising:

providing the enterprise address associated with the user to the VPN client.

21. The apparatus of claim 20, further comprising:

authenticating the VPN client prior to providing the enterprise address associated with the VPN client to the VPN client.

22. A computer readable medium comprising computer code for allowing VPN based mobile communications in a network having a VPN server and a VPN client, the computer readable medium comprising:

computer code for receiving a first message from the VPN client, the first message having a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address;

computer code for maintaining an association between the enterprise address and the VPN client,

computer code for receiving a second message from the VPN client, the second message having a second address associated with a second subnetwork as the source address and the enterprise address as the encapsulated address, wherein using the same enterprise address allows VPN based mobile communications when a VPN client moves from the first subnetwork to the second subnetwork.

23. The computer readable medium of claim 22, further comprising:

computer code for providing the VPN client with an access list identifying one or more destinations that can be accessed through the VPN server.

24. The computer readable medium of claim 22, wherein the first and second messages are associated with an established VPN tunnel.

25. The computer readable medium of claim 22, wherein the encapsulated address but not the source address is encrypted.

26. The computer readable medium of claim 22, wherein the enterprise address is a private network IP address.

27. The computer readable medium of claim 22, wherein using the same enterprise address allows VPN based mobile communications to continue seamlessly.

28. The computer readable medium of claim 22, wherein maintaining an association between the enterprise address and the VPN client comprises associating the enterprise address with a username.

29. The computer readable medium of claim 28, wherein the enterprise address is further associated with a password.

30. The computer readable medium of claim 22, further comprising:

computer code for providing the enterprise address associated with the user to the VPN client.

31. The computer readable medium of claim 30, further comprising:

computer code for authenticating the VPN client prior to providing the enterprise address associated with the VPN client to the VPN client.

32. A method for allowing communication in a network having a VPN server and a VPN client, the method comprising:

transmitting a first message to the VPN server with a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address;

detecting a change in location of the VPN client from the first subnetwork to a second subnetwork;

transmitting a second message to the VPN server with a second address associated with the second subnetwork as the source address and the enterprise address as the encapsulated address, wherein encapsulating the same enterprise address allows communication when a VPN client moves from a first subnetwork to a second subnetwork.

33. The method of claim 32, further comprising:
sending authentication information to the VPN server; and
obtaining the enterprise address from the VPN server.

34. The method of claim 32, further comprising:
receiving an access list from the VPN server identifying one or more destinations that can be accessed through the VPN server.

35. The method of claim 34, wherein the second message is transmitted after determining that a first destination is on the access list.

36. The method of claim 35, wherein a third message is transmitted to a second destination not on the access list without encapsulating the enterprise address.

37. The method of claim 33, wherein obtaining the enterprise address is associated with an established VPN tunnel.

38. The method of claim 32, wherein the encapsulated address is encrypted.

39. The method of claim 32, wherein the enterprise address is a company network IP address.

40. The method of claim 32, wherein using the same enterprise address allows VPN based mobile communications to continue seamlessly.

41. The method of claim 32, wherein the enterprise address is associated with a username.

42. The method of claim 32, wherein the first and second addresses are IP addresses.

43. The method of claim 32, further comprising:
replacing the first address in a TCP/IP stack with the enterprise address.

44. The method of claim 43, further comprising:
after the change in location is detected, obtaining the second address;
wherein the enterprise address in the TCP/IP stack is not replaced with the second address.

45. The method of claim 43, further comprising:
storing the first address and the second address in an operating system.

46. The method of claim 43, further comprising:
storing the first address and the second address in a device driver.

47. The method of claim 43, wherein the change in location of the VPN client from a first subnetwork to a second subnetwork is detected without user intervention.

48. The method of claim 47, wherein the VPN client does not replace the enterprise address in the TCP/IP stack with the second subnetwork address upon detecting the change in location.

49. An apparatus for allowing communication in a network having a VPN server and a VPN client, the apparatus comprising:
memory,
a processor coupled to memory, the processor configured to transmit a first message to the VPN server with a first address associated with a first subnetwork as a source address and an enterprise address as an encapsulated address, detect a change in location of the VPN client from the first subnetwork to a second subnetwork and transmit a second message to the VPN server with a second address associated with the second subnetwork as the source address and the enterprise address as the encapsulated address, wherein encapsulating the same enterprise address allows communication when a VPN client moves from a first subnetwork to a second subnetwork.

50. The apparatus of claim 49, wherein the processor is further configured to send authentication information to the VPN server and obtain the enterprise address from the VPN server.

51. The apparatus of claim 49, wherein the processor is further configured to receive an access list from the VPN server identifying one or more destinations that can be accessed through the VPN server.

52. The apparatus of claim 51, wherein the second message is transmitted after determining that a first destination is on the access list.

53. The apparatus of claim 52, wherein a third message is transmitted to a second destination not on the access list without encapsulating the enterprise address.

54. The apparatus of claim 50, wherein obtaining the enterprise address is associated with an established VPN tunnel.

55. The apparatus of claim 49, wherein the encapsulated address is encrypted.

56. The apparatus of claim 49, wherein the enterprise address is a company network IP address.

57. The apparatus of claim 49, wherein using the same enterprise address allows VPN based mobile communications to continue seamlessly.

58. The apparatus of claim 49, wherein the enterprise address is associated with a username.

59. The apparatus of claim 49, wherein the first and second addresses are IP addresses.

60. The apparatus of claim 49, wherein the processor is further configured to replace the first address in a TCP/IP stack with the enterprise address.

61. The apparatus of claim 60, wherein the processor is further configured to obtaining the second address after the change in location is detected, wherein the enterprise address in the TCP/IP stack is not replaced with the second address.

62. The apparatus of claim 60, wherein the processor is further configured to store the first address and the second address in an operating system.

63. The apparatus of claim 60, wherein the processor is further configured to store the first address and the second address in a device driver.

* * * * *

EXHIBIT 1006

U.S. Patent No. 7,155,518 to *Forslow et al.*

("*Forslow*")

US007155518B2

(12) **United States Patent**
Forslöw

(10) **Patent No.: US 7,155,518 B2**
(45) **Date of Patent: Dec. 26, 2006**

(54) **EXTRANET WORKGROUP FORMATION ACROSS MULTIPLE MOBILE VIRTUAL PRIVATE NETWORKS**

(75) Inventor: **Jan Forslöw**, Stockholm (SE)

(73) Assignee: **Interactive People Unplugged AB**, Stockholm (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 894 days.

(21) Appl. No.: **09/755,027**

(22) Filed: **Jan. 8, 2001**

(65) **Prior Publication Data**

US 2002/0133534 A1 Sep. 19, 2002

(51) **Int. Cl.**
G06F 15/16 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **709/227**; 709/205; 709/238; 709/223; 455/461

(58) **Field of Classification Search** 709/238, 709/242–249, 227, 250, 223, 201, 205; 370/251, 370/252, 401, 329, 352, 390; 455/403, 461, 455/451
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,445,920 B1 * 9/2002 Pfundstein 455/422.1
6,539,483 B1 * 3/2003 Harrison et al. 713/201
6,571,289 B1 * 5/2003 Montenegro 709/227
6,594,704 B1 * 7/2003 Birenback et al. 709/238
6,734,699 B1 * 5/2004 Herr et al. 326/1
6,778,494 B1 * 8/2004 Mauger 370/230
6,954,790 B1 * 10/2005 Forslow 709/227
6,977,938 B1 * 12/2005 Alriksson et al. 370/401
6,980,524 B1 * 12/2005 Lu et al. 370/254
2001/0033556 A1 * 10/2001 Krishnamurthy et al. ... 370/329

OTHER PUBLICATIONS

"Ad Hoc On-Demand Distance Vector (AODV) Routing" -by Perkins, Royer, Das, Oct. 22, 1999.*

* cited by examiner

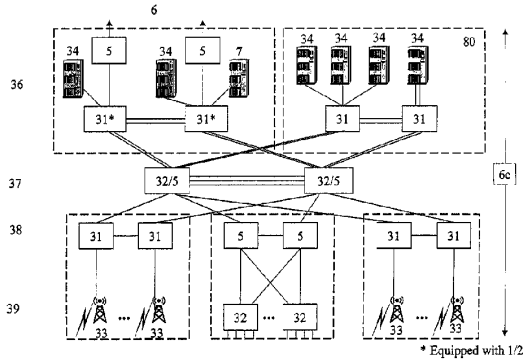
Primary Examiner—Jeffrey Pwu
(74) *Attorney, Agent, or Firm* Banner & Witcoff, Ltd.

(57) **ABSTRACT**

The present invention describes a network-based mobile workgroup system allowing a selected set of users from two or more mobile virtual private networks to form an extranet workgroup in a secure manner. The invention is based on the limited private address scenario, which entitles mobile nodes having private, possibly overlapping, addresses as defined in RFC 1918, while home and foreign agents have public IP addresses. Each home agent is dedicated to one mobile virtual private network (M-VPN), while a foreign agent may be shared by multiple M-VPNs. The system also entails a mobile service manager that has a public IP address and a set of mobile nodes that all have a UFQDN (user fully qualified domain name) within the overall mobile workgroup system.

The main benefits, compared to existing solution for extranet workgroup creation, are that extranets can be created despite overlapping address realms. Even fine-granular workgroups within the extranet can be created with any set of users from any set of M-VPNs. The mobility aspect of the M-VPN fits well for supporting peer-to-peer applications, such as voice over IP, between mobile clients. Although the mobile clients may belong to different M-VPNs, with different address realms, per packet authentication and filtering is always possible to perform by the ingress M-VPN security gateway using a realm-indexed filtering technique. Finally, the responsibility for allocating resources, to be reached by an extranet workgroup, is completely delegated to each M-VPN.

29 Claims, 18 Drawing Sheets



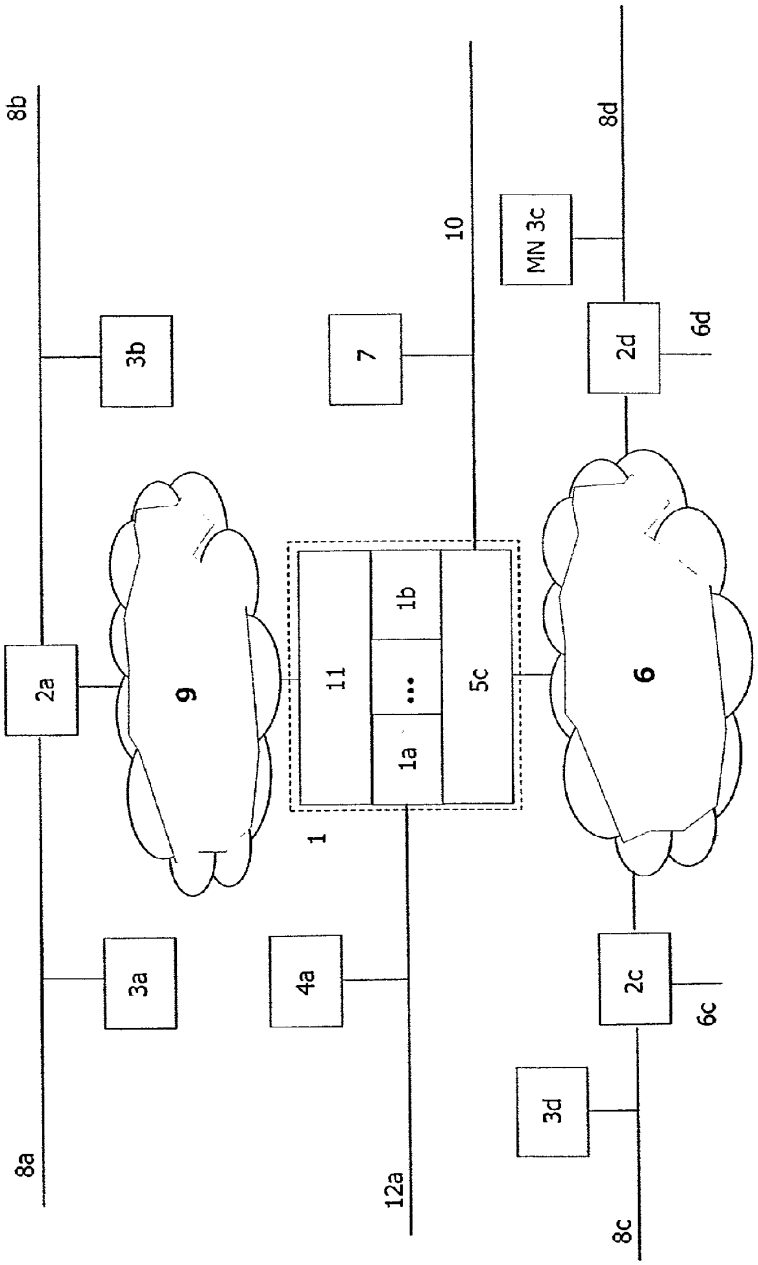


Fig. 1

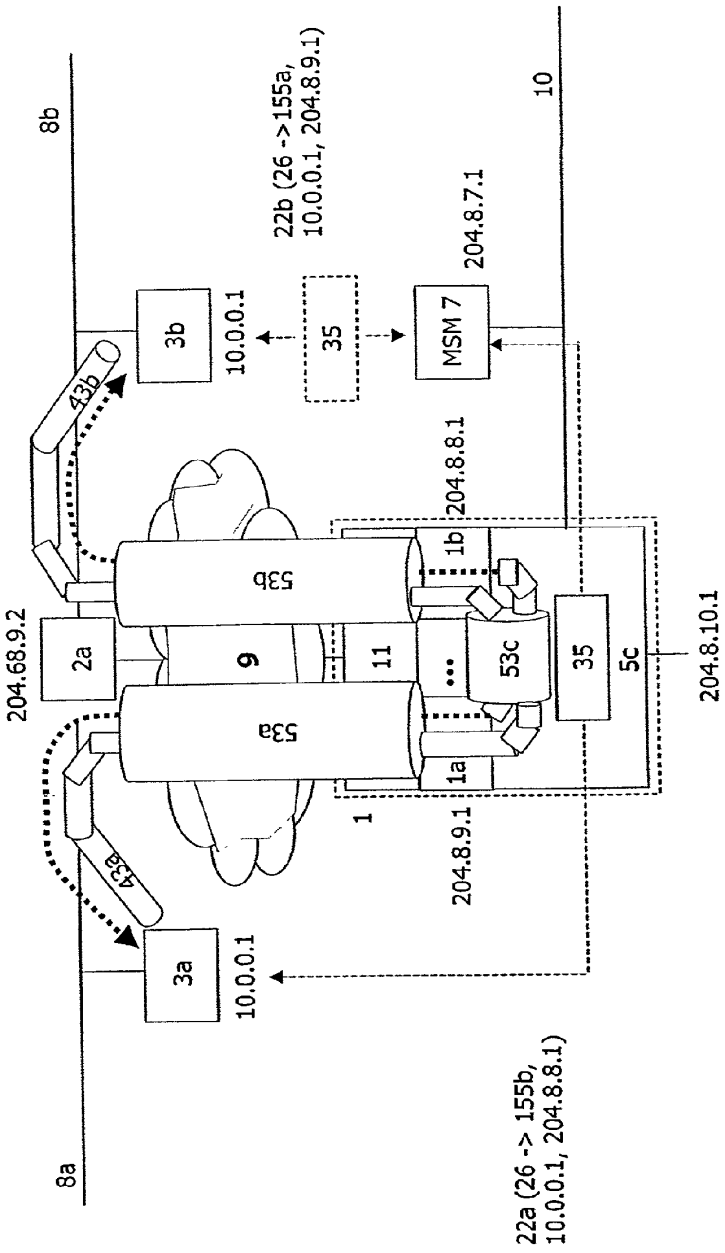


Fig. 2

AA/SWA Ex. 1015, p.108 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

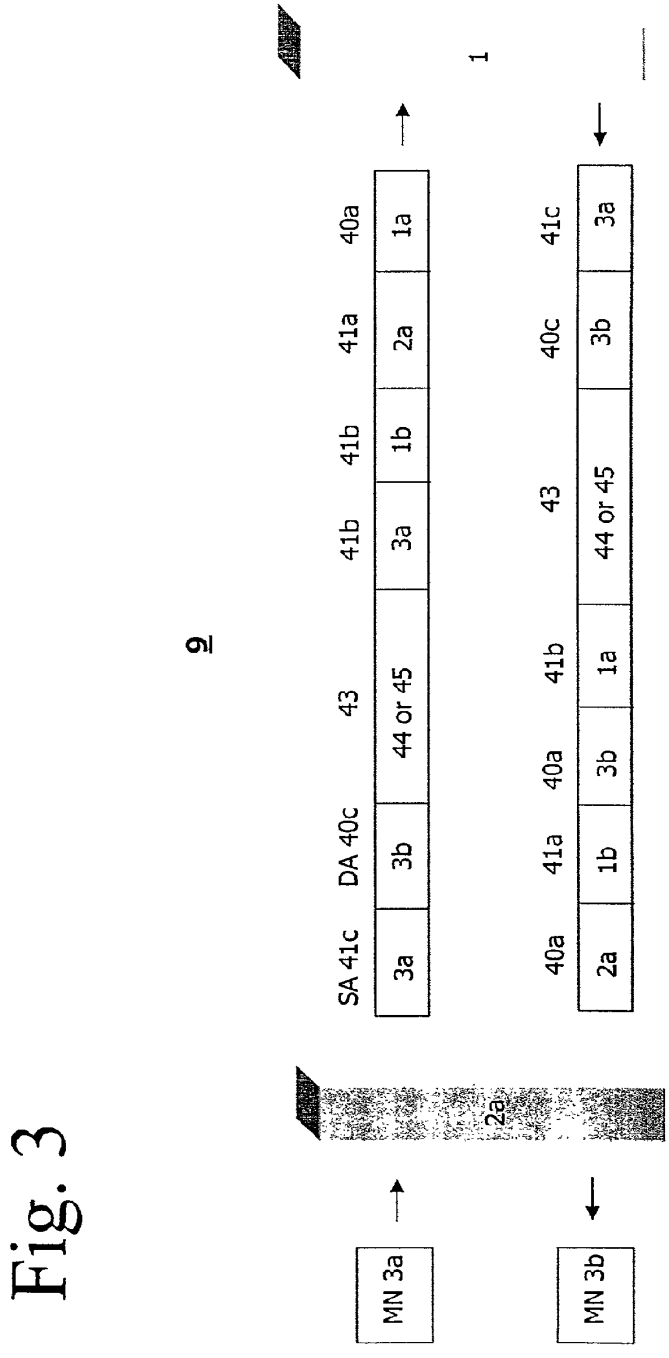


Fig. 3

AA/SWA Ex. 1015, p.109 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

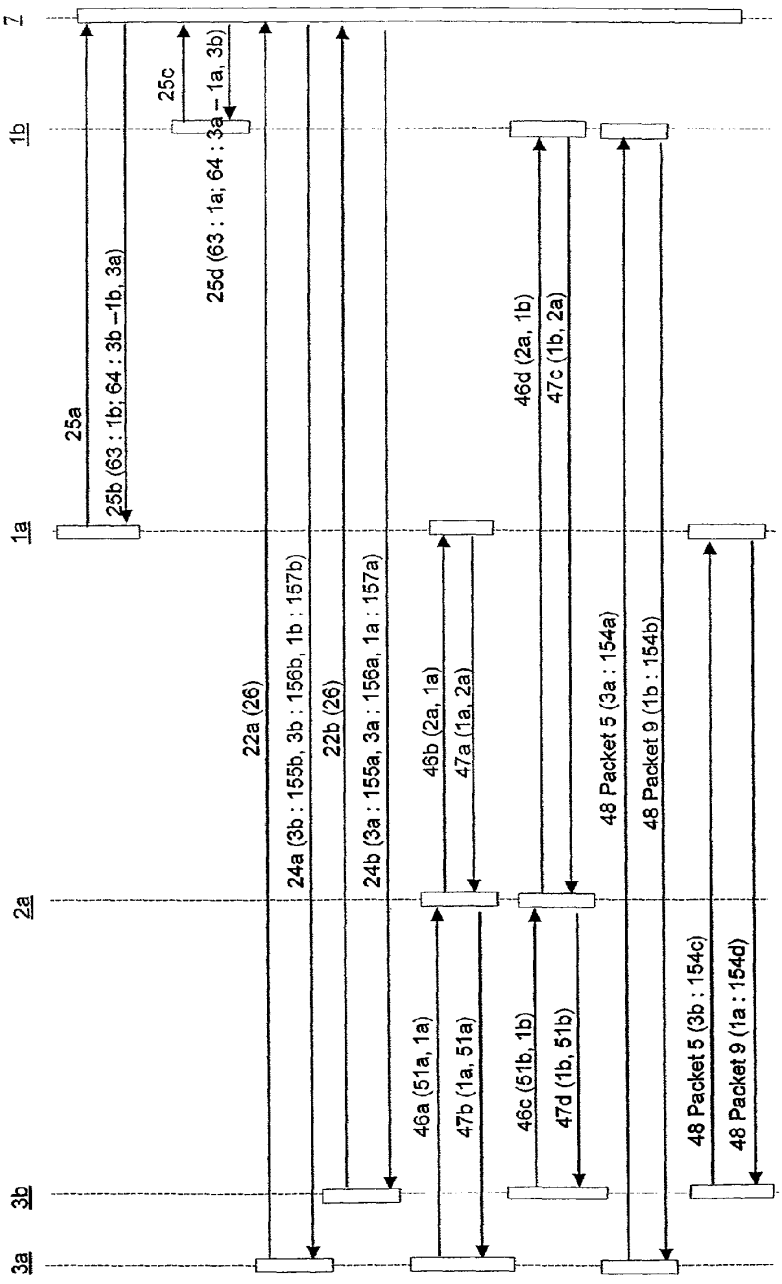


Fig. 4a

AA/SWA Ex. 1015, p.110 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

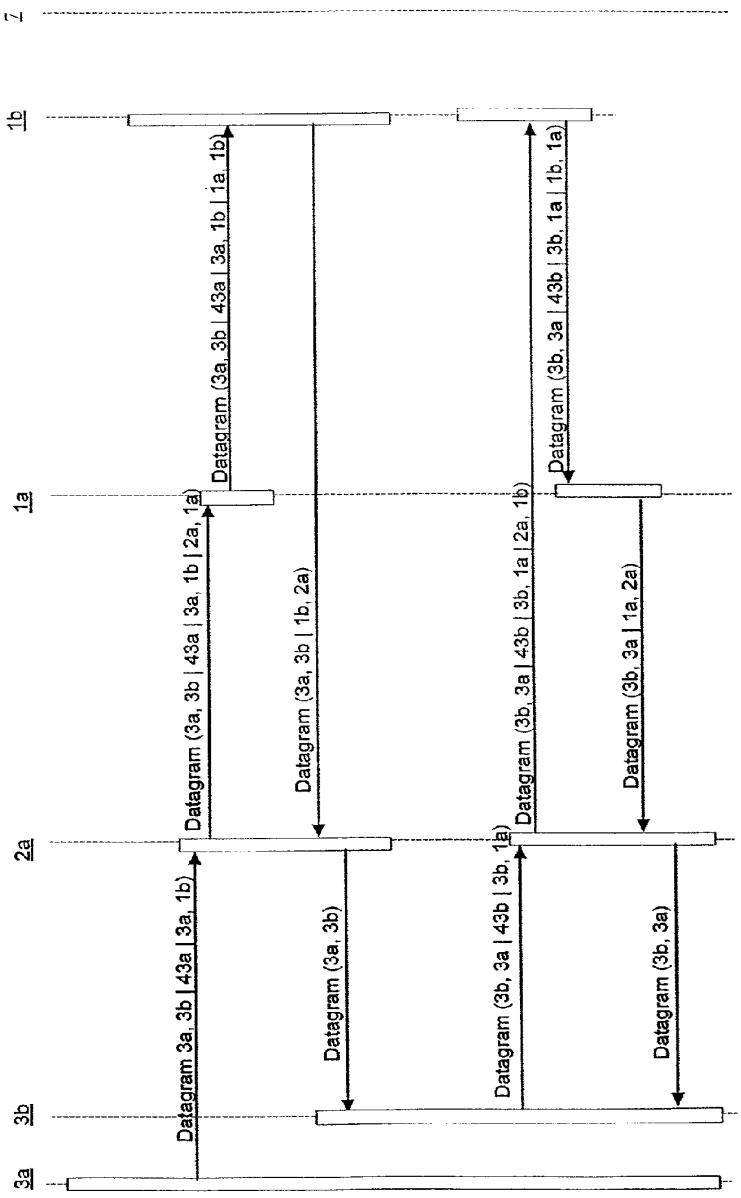

1b
1a
2a
3b
3a
Datagram (3a, 3b | 43a | 3a, 1b | 1a, 1b)
Datagram (3a, 3b | 43a | 3a, 1b | 2a, 1a)
Datagram (3a, 3b | 1b, 2a)
Datagram 3a, 3b | 43a | 3a, 1b)
Datagram (3a, 3b)
Datagram (3b, 3a | 43b | 3b, 1a | 1b, 1a)
Datagram (3b, 3a | 43b | 3b, 1a | 2a, 1b)
Datagram (3b, 3a | 1a, 2a)
Datagram (3b, 3a | 43b | 3b, 1a)
Datagram (3b, 3a | 43b | 3b, 1a)
Datagram (3b, 3a)

Fig. 4b

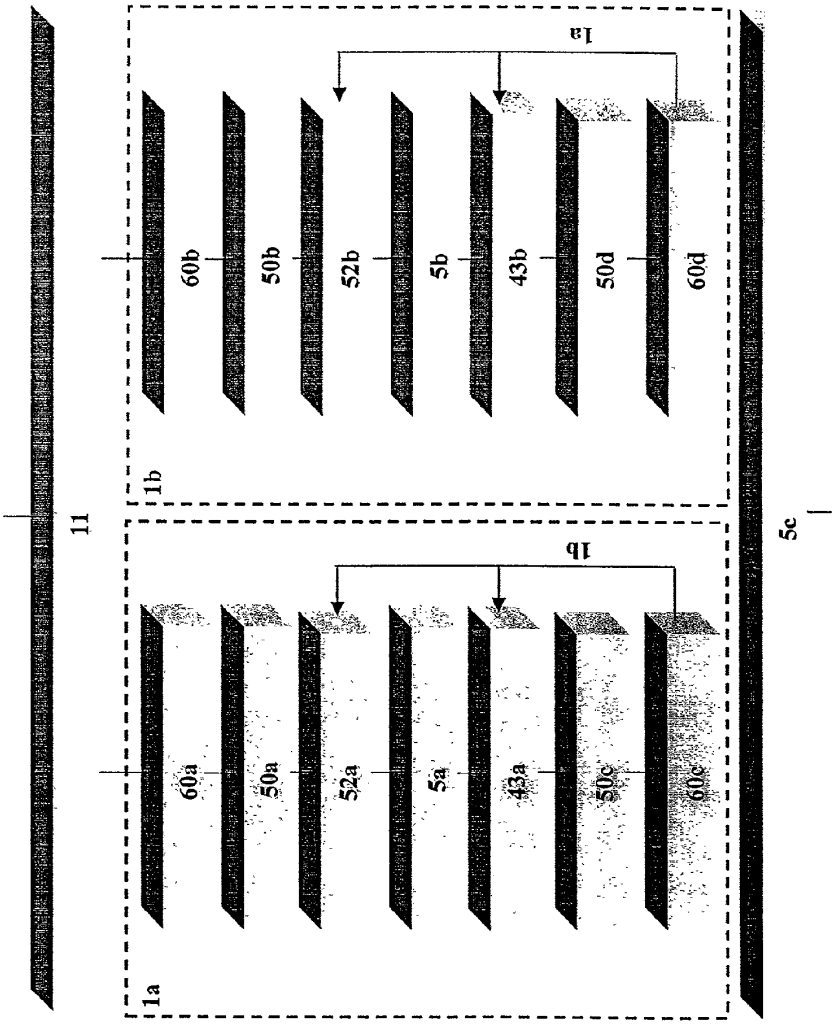

1a
60b
50b
52b
5b
43b
50d
60d
1b
11
1b
60a
50a
52a
5a
43a
50c
60c
1a
5c

Fig. 5

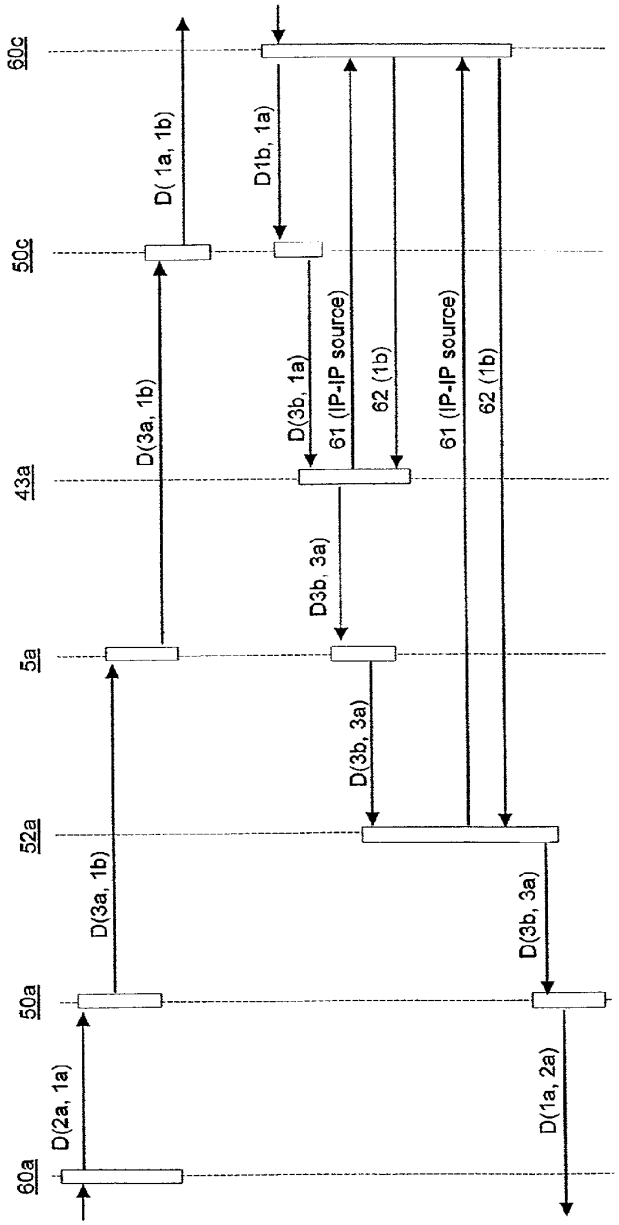

60c
50c
43a
5a
52a
50a
60a
D(1a, 1b)
D1b, 1a)
D(3a, 1b)
D(3b, 1a)
61 (IP-IP source)
62 (1b)
61 (IP-IP source)
62 (1b)
D3b, 3a)
D(3b, 3a)
D(3a, 1b)
D(3b, 3a)
D(2a, 1a)
D(1a, 2a)

Fig. 6a

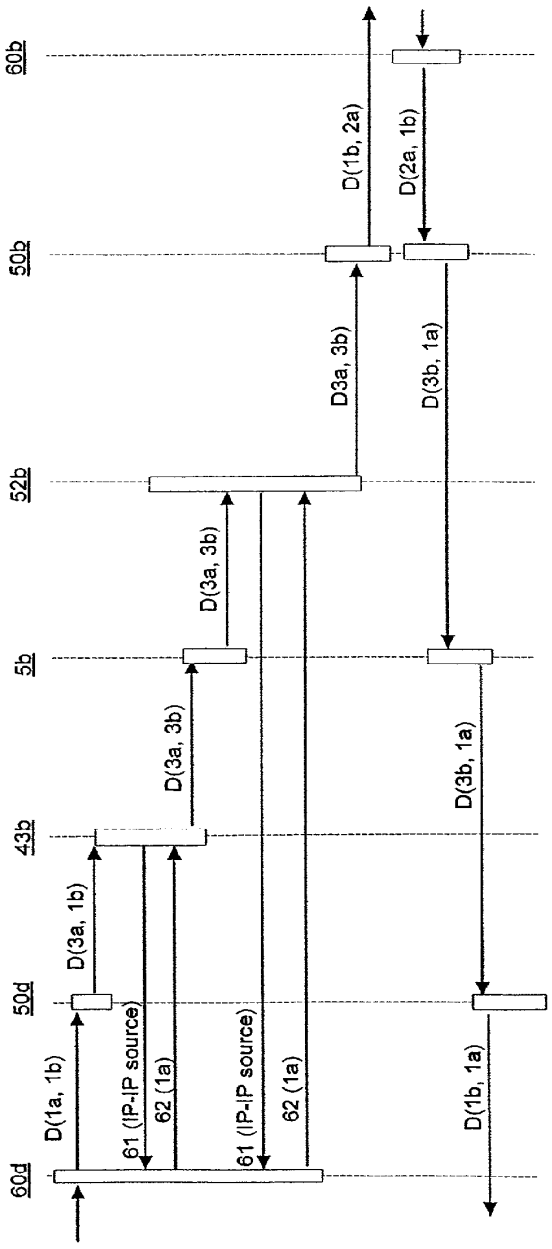
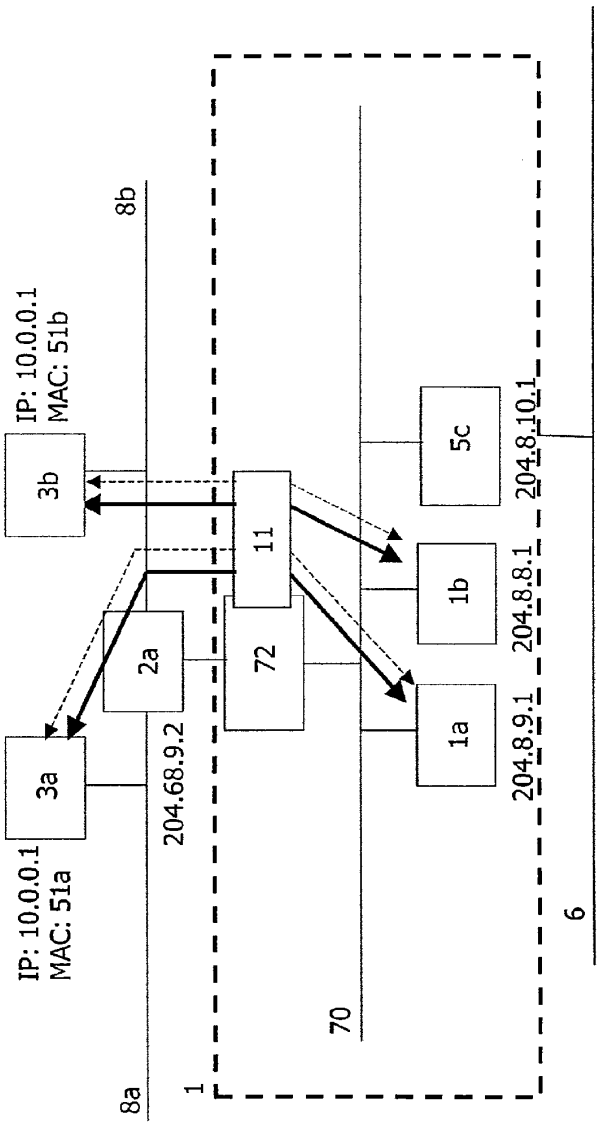

60b
50b
52b
5b
43b
50d
60d
D(1b, 2a)
D(2a, 1b)
D3a, 3b)
D(3b, 1a)
D(3a, 3b)
D(3a, 3b)
D(3b, 1a)
D(3a, 1b)
D(1a, 1b)
61 (IP-IP source)
62 (1a)
61 (IP-IP source)
62 (1a)
D(1b, 1a)

Fig. 6b

Fig. 7



AA/SWA Ex. 1015, p.115 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

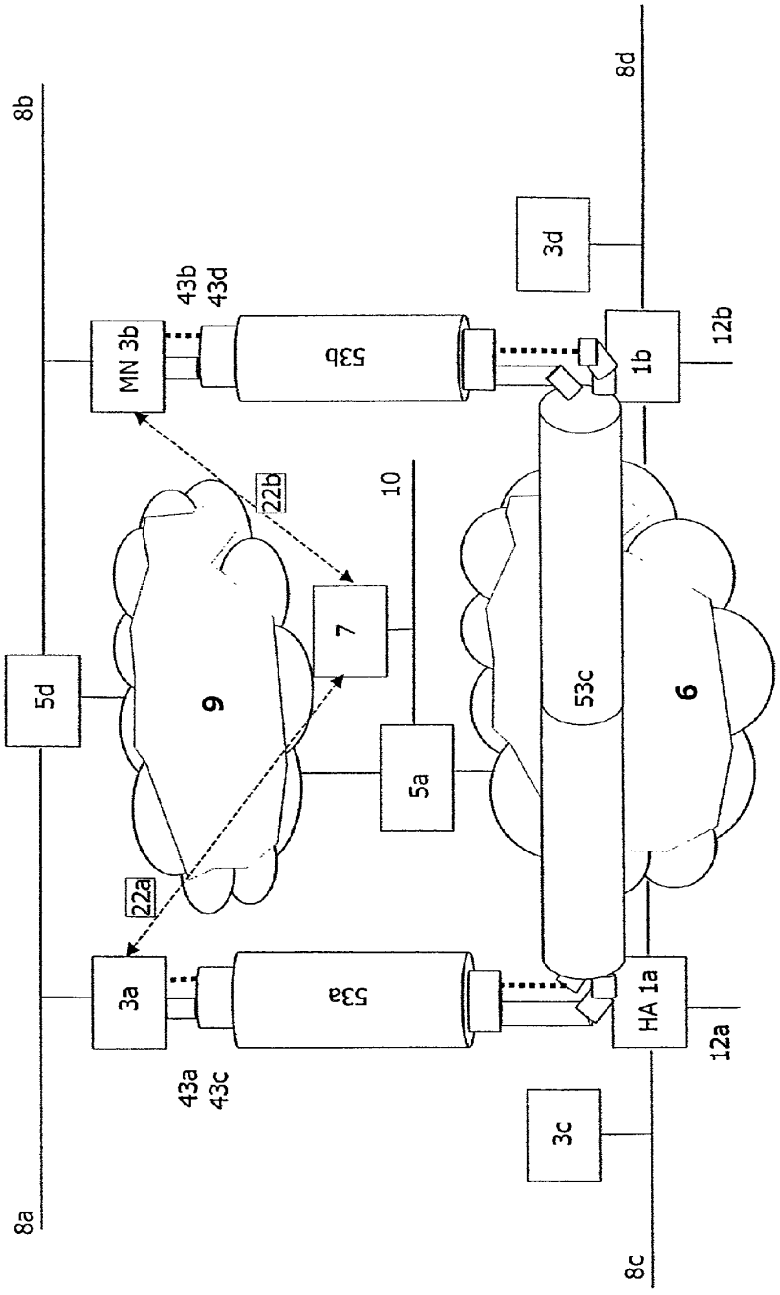

8b
8d
3d
43b
43d
MN 3b
53b
1b
12b
22b
10
7
5d
9
53c
6
5a
22a
3a
53a
HA 1a
12a
43a
43c
3c
8a
8c

Fig. 8

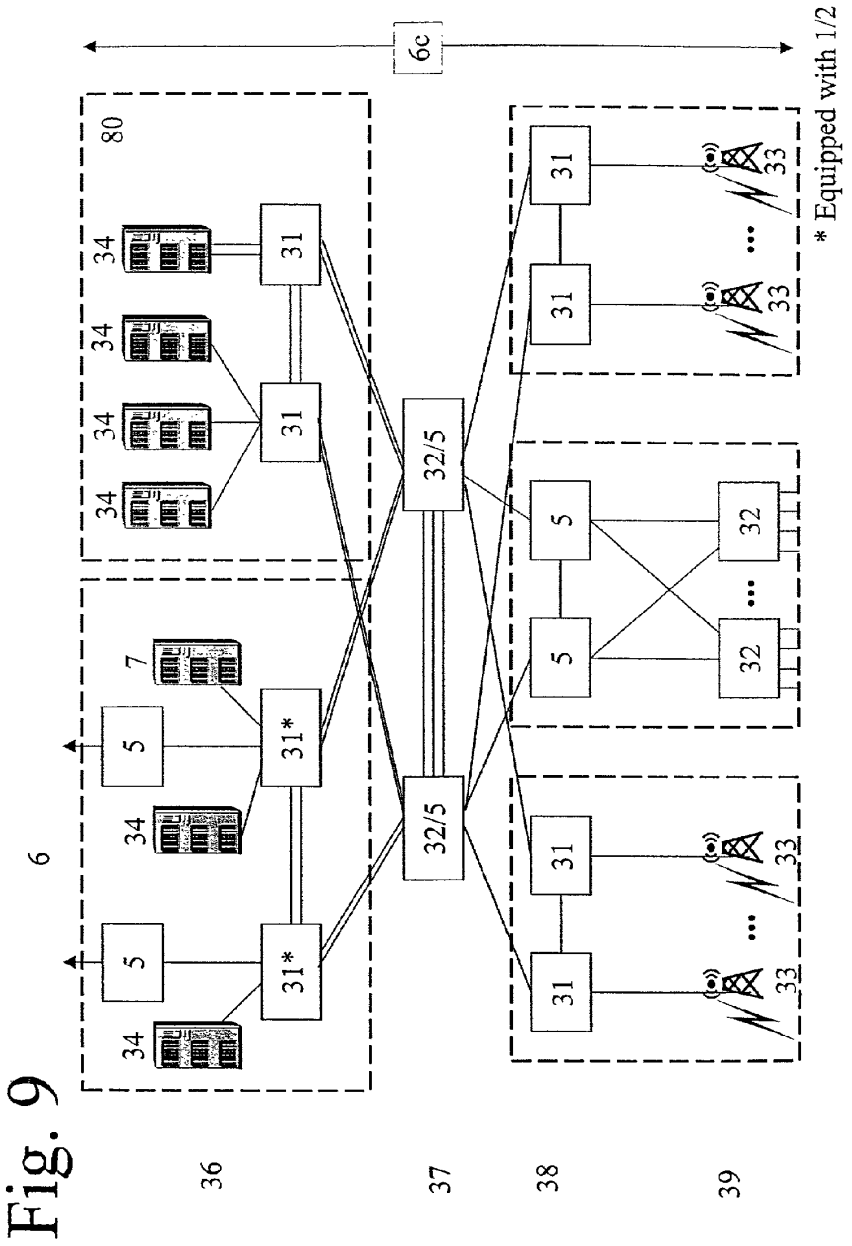


Fig. 9

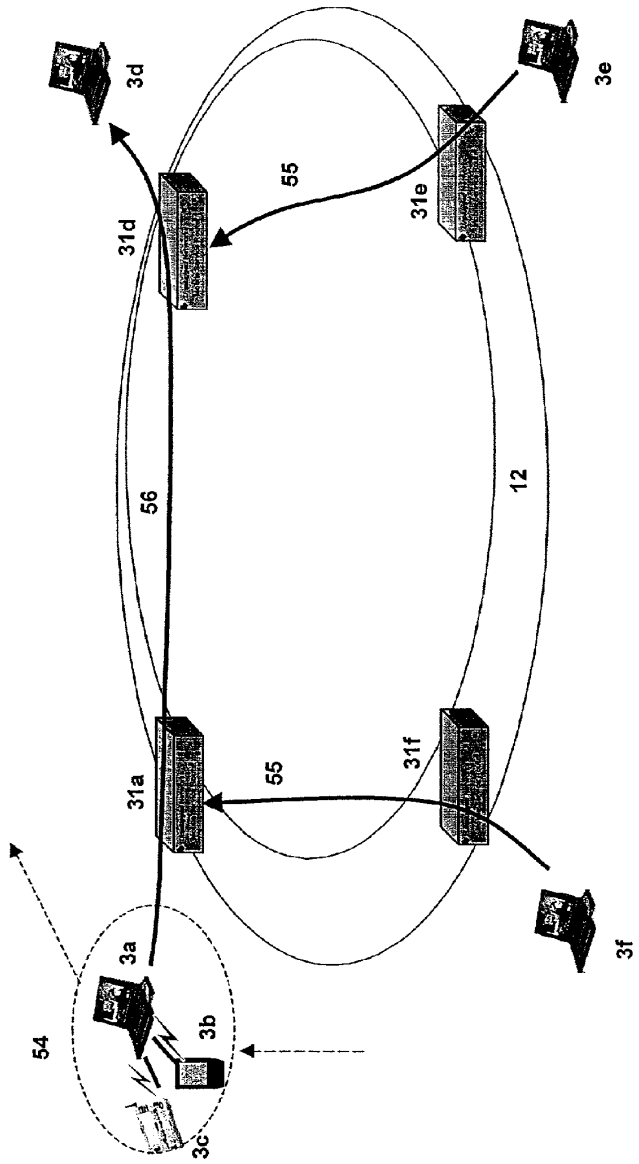


Fig. 10a

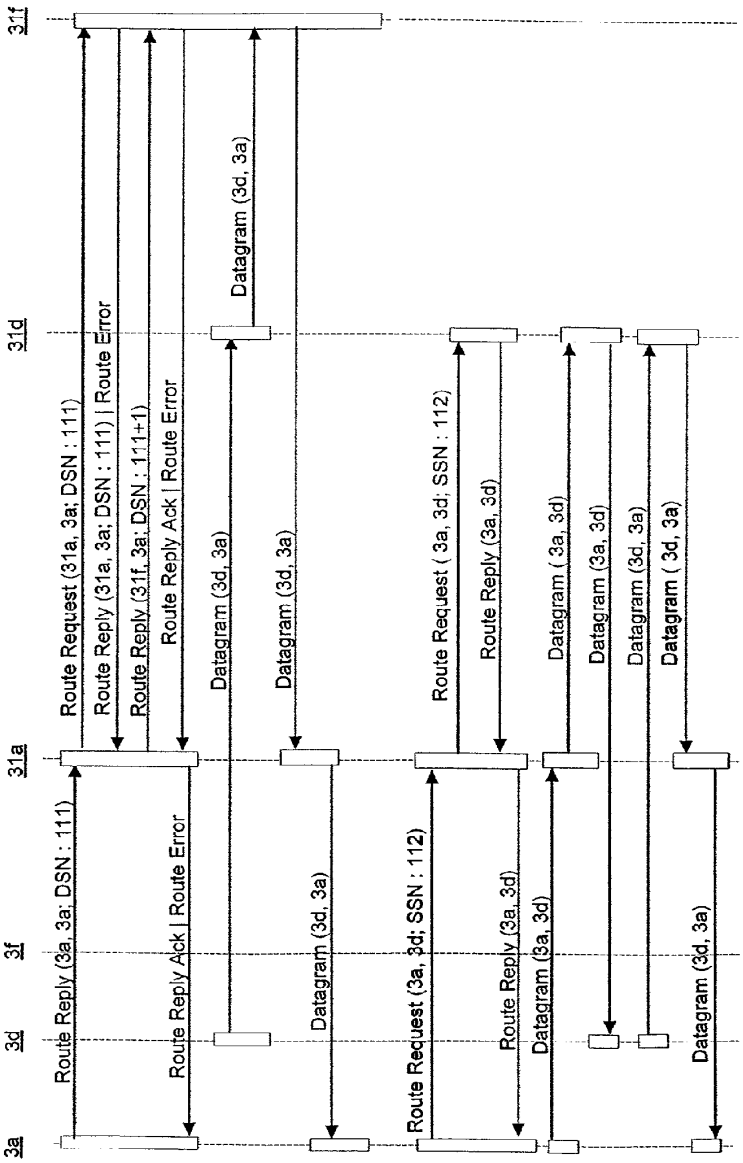


Fig. 10b

AA/SWA Ex. 1015, p.119 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

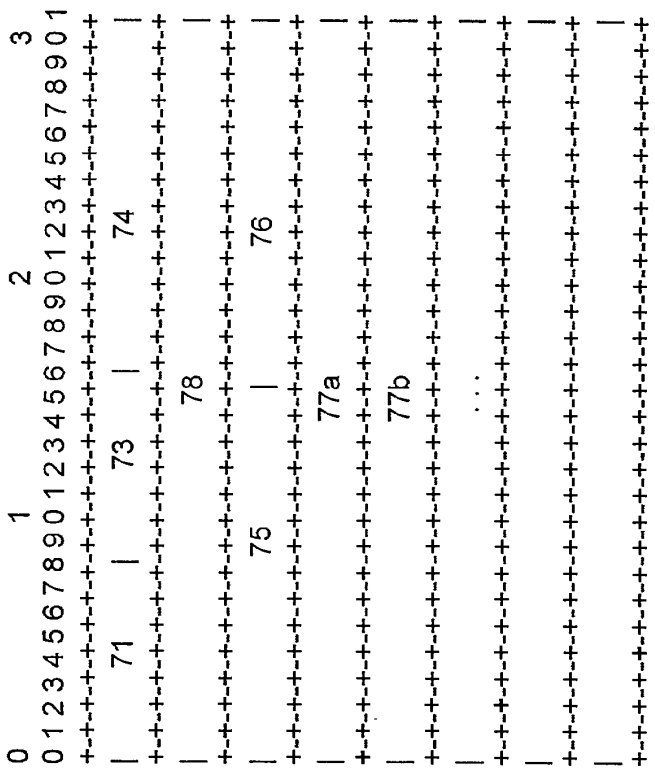


Fig. 10c

AA/SWA Ex. 1015, p.120 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

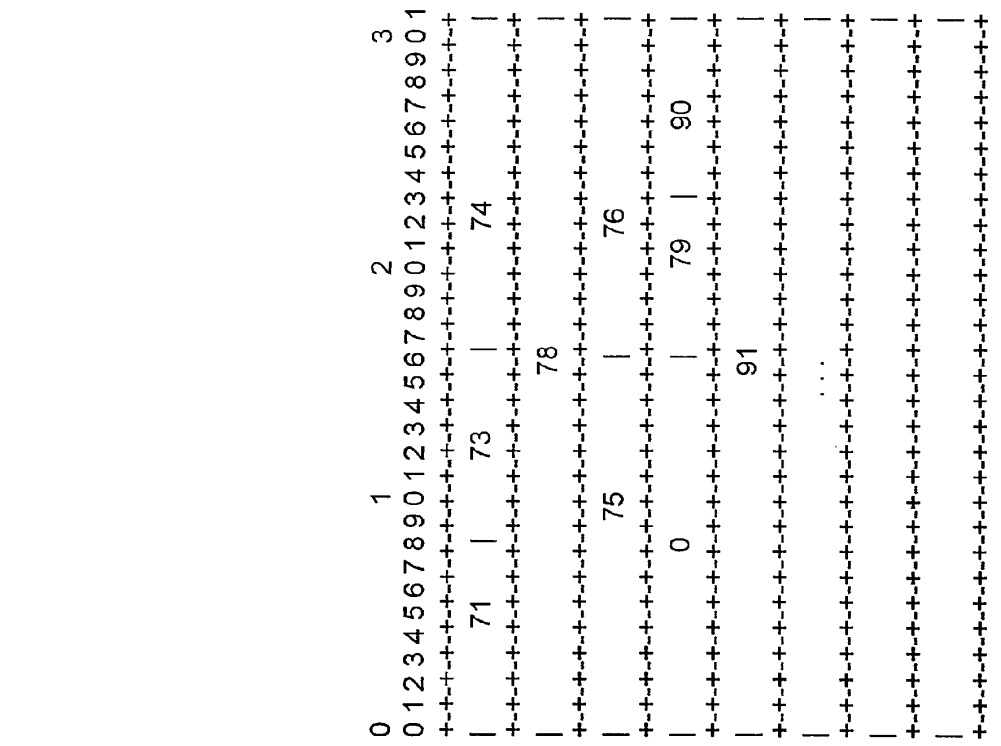

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
71
73
74
78
75
76
0
79
90
91

Fig. 10d

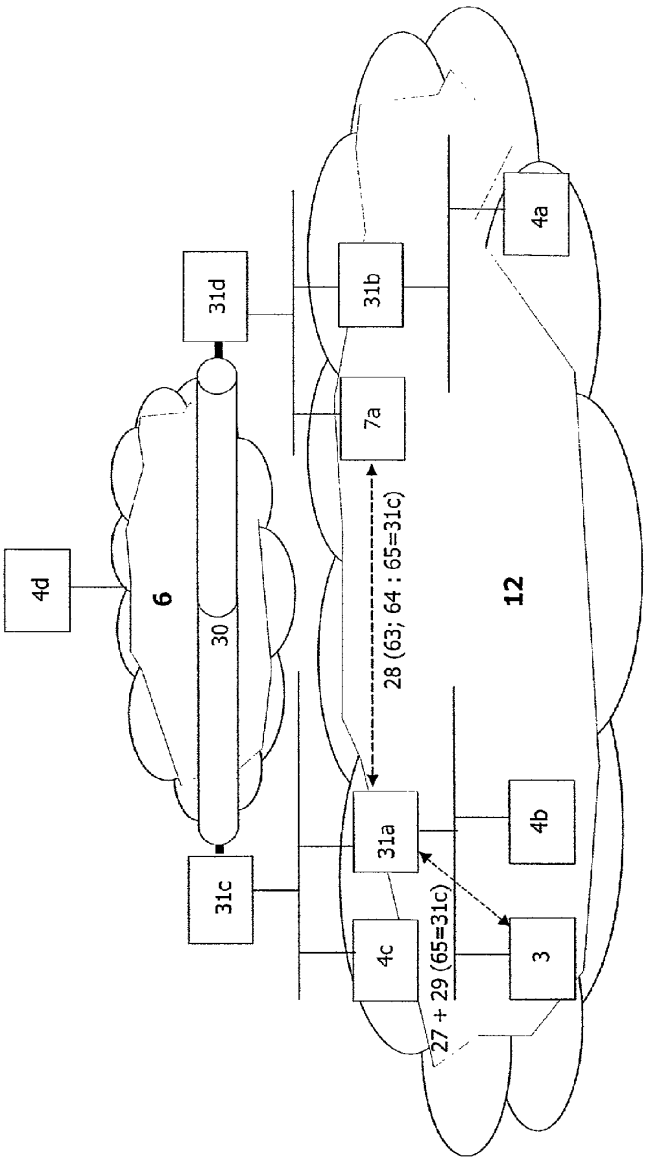


Fig 11

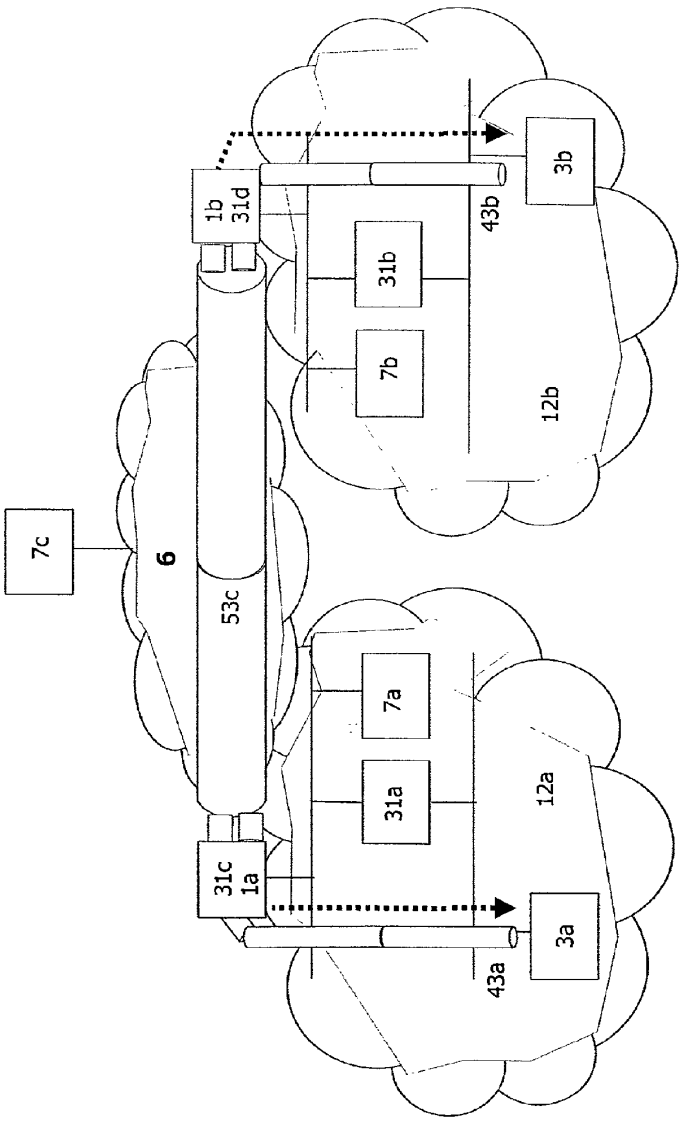


Fig. 12a

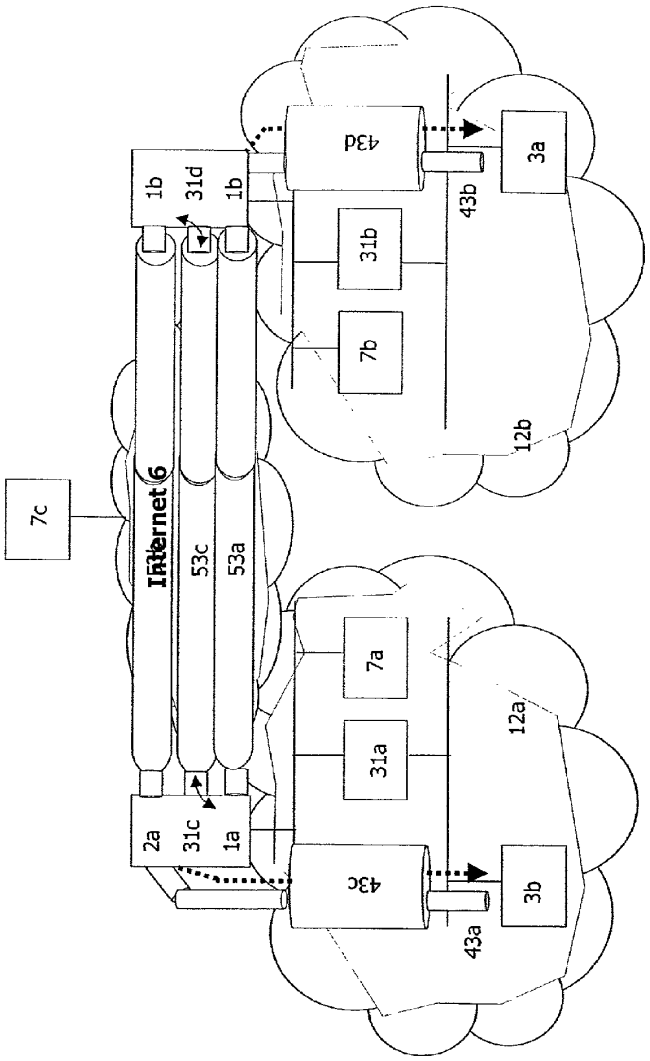

1b
31d
1b
43d
3a
43b
31b
7b
12b
7c
Internet 6
53c
53a
7a
12a
31a
2a
31c
1a
43c
3b
43a

Fig. 12b

EXTRANET WORKGROUP FORMATION ACROSS MULTIPLE MOBILE VIRTUAL PRIVATE NETWORKS

FIELD OF THE INVENTION

The present invention relates to mobile data communications in general. More specifically, the present invention describes a network-based mobile workgroup system allowing a selected set of users from two or more mobile virtual private networks to form an extranet workgroup in a secure manner.

BACKGROUND AND SUMMARY OF THE INVENTION

The following definitions are introduced for the purpose of clarity.

AAA Authentication, Authorization and Accounting: AAA is a common name for both RADIUS and DIAMETER, i.e. solutions providing customer care, control and billing in a large IP network.

DIAMETER: A successor of RADIUS with increased security and scalability features compared to its predecessor RADIUS. It is currently under standardization by the IETF.

DHCP: Dynamic Host Configuration Protocol. DHCP is an Internet Engineering Task Force (IETF) standard for allocating Internet Protocol addresses and other configuration information to User Systems. User Systems can either be Fixed Hosts or Mobile Hosts. The allocation is done each time when the User System is started. A DHCP server allocates the information, which is then transferred to a DHCP client. An Internet Service Provider or an IT-department controls the DHCP server. The DHCP client is a SW functionality embedded in the User System.

DMZ: De-Militarized Zone is a zone between the Internet Service Provider router and Corporate firewall where access is allowed from both the Internet and the Intranet. Normally a subset of the services available on the Intranet is mirrored on the DMZ.

FA: Foreign Agent. The primary responsibility of an FA is to act as a tunnel agent which establishes a tunnel to a HA on behalf of a mobile node in a mobile IP environment.

HA: Home Agent. The primary responsibility of the HA is to act as a tunnel agent which terminates the mobile IP tunnel, and which encapsulates datagrams to be sent to the Mobile Node in mobile IP.

IETF: Internet Engineering Task Force. The IETF is the standardization organization for the Internet community.

IP: Internet Protocol. IP is a network layer protocol according to the ISO protocol layering. IP is the major end-to-end protocol between Mobile and Fixed End-Systems for Data Communications.

MANET: Mobile Ad hoc Networks. MANET is a common name for a family of protocols that provide multi-hop routing in highly dynamic mobile environments.

MIP: Mobile IP. MIP is an IP mobility standard being defined by the IETF with the purpose to make IP networks mobility aware, i.e. providing IP entities knowledge on where a Mobile Node is attached to the network. The standard includes the definition of a Foreign Agent and a Home Agent.

MN: Mobile Node. The MN comprises both the Terminal Equipment (TE) and the Mobile Termination (MT).

VLAN: Virtual Local Area Network. VLAN is a separation of a physical Local Area Network into a set of logical subnets.

VPN: Virtual Private Network. VPN is a secure overlay network on a common public infrastructure that allows a corporation to maintain its own addressing and routing between its sites and to remote users.

WLAN: Wireless Local Area Network. WLAN is a local area solution for radio access mobility for Mobile Nodes.

The business communication process consisting of suppliers, customers and partners are getting more and more interlaced. Even if business-to-business communication is in the midst of its hype, and the reality may not be as glamorous as first described, the needs for such solutions will remain. Extranets will play an important role of customer relationship management in the future.

However, as the security consciousness increase in organizations, it is not satisfactorily to just tie two or more companies together into an extranet. One would like to form workgroups within this extranet in order to create smaller zones-of-trust, allowing only a set of people to have access to a set of resources. This development has got increased focus as studies, such as the 2000 CSI-FBI Computer Crime and Security Survey, indicate that more than 70% of all unauthorized access to confidential information is made from the inside (i.e. not from the Internet). These types of computer crimes are by far the most expensive of all computer crimes within an enterprise.

There are essentially two network types where one can include support for extranet solutions. One is in the virtual private network that connects sites together and the other is in the campus networks of each site. The current best practice for both these network types are explained in the following chapter.

Several solutions have been put forward to achieve different levels of network privacy when building VPNs across a shared IP backbone, so target network-based VPNs. Most of these solutions require separate per VPN forwarding capabilities and make use of IP or MPLS based tunnels across the backbone network. The state of the art when it comes to providing extranets in network-based VPNs is to deploy of a set of virtual routers (VRs) in one physical router. In this sense both intranet and extranet VPNs can be deployed, each using a separate virtual router. The objective is to provide per VPN based routing, forwarding, quality of service, and service management capabilities. The virtual router concept deploys exactly the same mechanisms as a physical router, and therefore inherits all existing mechanisms and tools for configuration, deployment, operation, troubleshooting, monitoring, and accounting. Virtual routers can be deployed in different VPN configurations, direct VR to VR connectivity through layer-2 links/tunnels or by aggregating multiple VRs into a single VR combined with IP or MPLS based tunnels. This architecture accommodates different backbone deployment scenarios, e.g. where the VPN service provider owns the backbone, but also where the VPN service provider obtains backbone service from one or more other service providers.

Within a VPN domain, an instance of routing is used to distribute VPN reachability information among VR routers. Any routing protocol can be used, and no VPN-related modifications or extensions are needed to the routing protocol for achieving VPN reachability. VPN reachability information to and from customer sites can be dynamically learned from the customer equipment using standard routing protocols or it can be statically provisioned on the VR. The routing protocol between the virtual routers and customer equipments is independent of the routing used in the VPN backbone. Furthermore, the routing protocol between the

AA/SWA Ex. 1015, p.125 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

VRs may be the same or it might be different than the routing mechanism used between the customer equipment and the VR.

There are two fundamental architectures for implementing network based VPNs. Those are virtual routers (VR) and piggybacking. The main difference between the two architectures resides in the model used to achieve VPN reachability and membership functions. In the VR model, each VR in the VPN domain is running an instance of a routing protocol responsible to disseminate VPN reachability information between VRs. Therefore, VPN membership and VPN reachability are treated as separate functions, and separate mechanisms are used to implement these functions. VPN reachability is carried out by a per-VPN instance of routing, and a range of mechanisms is possible for determining membership. In the piggyback model the VPN network layer is terminated at the edge of the backbone, and a backbone routing protocol (i.e. BGP-4) is responsible for disseminating the VPN membership and reachability information between provider edge routers (PE) for all the VPNs configured on the PE.

Extranets are commonly used to refer to a scenario whereby two or more companies have network access to a limited amount of each other's corporate data. An important feature of extranets is the control of who can access what data, and this is essentially a policy decision. Policy decisions are enforced at the interconnection points between different domains. The enforcement may be done via a firewall, router with access list functionality, or any device capable of applying policy decision to transit traffic.

In the VR architecture, policy is enforced between two VPNs, or between a VPN and the Internet, in the same manner as is done today without VPNs. For example, two VRs (VPNs) could be interconnected. Each VR locally imposes its own policy controls via a firewall on all traffic that enters its VPN from the outside (whether from another VR or from the Internet). Combining firewalls and exchanging private routes between VRs (members of different VPNs) provide a mechanism to build different flavors of extranets. However, this network-based VPN model has some drawbacks or flaws:

- a Corporations normally apply private address realms in the VPNs, and creating an extranet VPN by tying together two existing VRs, would then create address collisions. Therefore, in this model, each new extranet normally a new set of virtual routers with a separate address realm from any of the intranet VPNs has to be created. This does not only mean an exponential increase in the number of virtual routers, but also that the end stations are required to be associated with at least one IP address for every VPN (intranet and extranet) that it belongs to.
- It is not clearly defined in current network-based VPN models, how security associations, user authentication and ingress filtering is performed of an extranet end station trying to reach a resource or a workgroup member from another partner company.
- The extranet VPN does not take into account the primary access network available to companies, namely their own campus networks. It is natural to think that partner companies will visit each other's sites quite frequently and would therefore like to have the same extranet VPN workgroup access policy apply also internally in the campus network.

This brings us naturally to the question on how workgroups can be applied in campus networks. The current best practice in campus network design is denoted the multilayer model. The multilayer model is designed to encompass the increased usage of central server farms. The traffic pattern in this model is based on having 20 percent of the traffic local to the workgroup LAN and 80 percent of the traffic leaving the workgroup (primarily towards the server farm).

The multilayer model consists of an access, distribution, core and core distribution layer. The access layer is typically based on layer 2 Ethernet switches, each hosting a number of virtual LANs (VLANs). Each virtual LAN is restricted to about 30 employees in order to limit broadcast radiation and broadcast interrupts on end-stations. A typical access layer switch (also called closet node) can host several VLANs, but is often limited to max 100 users. This typically covers one floor in a building. The capacity of today's Ethernet switches is really much higher than the aggregate throughput requirements of 100 users. The reason to limit the number of users to about 100 is primarily related to the impact an access node failure would have on the company as whole or its employees' productivity to be more exact.

The distribution nodes are multilayer switches (layer 2 and 3). Each access layer switch is interconnected to two distribution nodes in order to provide redundancy in case of link failure. As the normal Spanning Tree Protocol (STP) has slow convergence (about 40–50 seconds), most vendors have introduced own schemes (like the UplinkFast feature in Cisco's Catalyst 5000) in order to shorten the VLAN failover time to something like a few seconds. The UplinkFast feature is only applied between two neighbor distribution nodes and is, therefore, not applicable for network-wide redundancy solution. If a switched link layer solution shall be applied for redundancy throughout the network then STP has to be used again. However, generally routing protocols have a better convergence time and are therefore preferred as the network-wide redundancy solution. As an example, OSPF is normally applied to achieve network-wide redundancy in the distribution and core layer. In a big campus network, a building constitutes an OSPF area and the distribution node becomes an area border router to the OSPF backbone. In addition, VRRP or HSRP is applied between two neighbor distribution nodes for the purpose of network layer redundancy towards an access node.

VLAN trunking of individual user VLANs is performed at the access node in order to gather all workgroup LAN access control to the distribution node. VLAN trunking may use an Ethernet Channel (multiple FastEthernet) or a GigEthernet link. The identification in the Access Control List (ACL) is based on VLAN port and MAC address.

The core network can either be based on layer 2 or "vanilla" layer 3 switching. The decision on what to choose is determined by the size of the OSPF backbone. The number of neighbors cannot be more than roughly 100 in current OSPF implementations. There may also be other considerations for segmenting the backbone into several VLANs, e.g. in order to separate management traffic from, RTP services, from HTTP services and so on.

Finally, a new set of distribution nodes are typically placed in front of the server farm and the WAN firewall DMZ respectively. All the server-to-server traffic is then kept off the backbone and VRRP can run in-between a core distribution pair for the purpose of failover protection. The core distribution nodes may also include access control lists.

Each pair of communicating distribution nodes has multiple equal-cost paths to each other. A campus IT-administrator ensures loadbalancing and redundancy from one distribution node to another across the core by running OSPF across these multiple equal-cost paths.

Current workgroup definitions in a campus network are based on the allocation of employees and their MAC addresses into virtual LANs. The user is tied to a LAN workgroup through the port number to which his MAC address is associated. The security restrictions are enforced using Access Control Lists (ACLs) on the distribution node interface towards the access layer.

A campus-wide VLAN model provides the flexibility to have statically configured end stations move to a different floor or building within the campus. When a user plugs-in his PC in a LAN port in another building, the local distribution node will send a query to a VLAN membership policy server to determine access policy and VLAN membership for the user. Then the distribution node adds the user's port to the appropriate VLAN. At the network layer, however, the end station is still required to get a new IP address that conforms to the route aggregation hierarchy of OSPF. This in turn will require the user to restart his session-based applications when changing floor or building.

Furthermore, an access control policy, that is limited to the case of Ethernet link connectivity between the end station and the distribution node, is not generally applicable. It is, e.g., not possible to apply in the case of accessing the Intranet from wide area networks (PPP or IPSec remote access) or via adhoc networks (like Bluetooth). A workgroup policy system based on network layer identities is on the other hand applicable to these cases as well

The success factors of extranets in campus networks lie in the provisioning of flexible access to and partial inclusion of personnel and servers in workgroups. This means that:

- Persons that shall be part of an extranet workgroup shall be possible to select down to the granularity of individuals;
- Server resources from all partners shall be possible to bring into the extranet workgroup; and
- Extranet workgroup participants shall be able to roam at both, or better any, corporate location while still being granted secure access to the resources and being reachable for other colleagues.

This means that extranet access shall be granted to members both from within the campus and from remote. One special case of the latter is when visiting one of the extranet partner's sites, at which time the workgroup member shall have access to both local and home resources allocated to the extranet workgroup.

So how does the multilayer model map to these requirements? The separation of the access layer from the server farm is a first step. However, the VLAN workgroup access control in the distribution layer is limited to the employees of the company. For extranets, there is a need for a policy management system that controls network resource usage in multiple companies. Furthermore, it is not likely that such an extranet management system will have a hook to every node in the distribution layer, but rather to specialized nodes at the DMZ. The distribution nodes will then need to be instructed to securely tunnel traffic to and from the visiting member up to a gateway node for authentication, filtering and selective tunneling back to the member's home office.

The closest resemblance of a gateway node like this is today's VPN routers. The VPN router can either apply IPSec and/or L2TP tunneling to another site. L2TP has the limitation of requiring link layer access between the end station and the L2TP Access Concentrator (LAC). IPsec is more generally applicable as it can encapsulate IP packets even in multihop access environments, as is the case in the campus environment.

IPSec-based VPN boxes may be instructed to route some traffic locally and other traffic through an IPSec tunnel to another site. Some of them are also equipped with good firewall functionality that is controlled from a central server. What they are lacking in terms of extranet support are:

- A management system that helps to decentralize management of extranet workgroups to the involved parties and individuals;
- A secure protocol that allows the local VPN gateway to request from the home VPN gateway authentication data on the mobile user and instructions on how to filter and route traffic based on destination and service type;
- A dynamic protocol that allows a VPN box to regularly authenticate the guest user to IP address mapping in a non-"service disruptive" fashion; and
- A NAT-function that can cope with overlapping address realms between members of the extranet, i.e. still providing a unique identity for reachability and filtering purposes.

The following references are also of general interest for the understanding of the present invention:

Bellur, Bhargav et al; Topology Broadcast based on Reverse-Path Forwarding (TBRPF); http://www.ietf.org/internet-drafts/draft-ietf-manet-tbrpf-00.txt; Jul. 2000

Calhoun, Pat et al; DIAMETER Base Protocol; http://www.ietf.org/internet-drafts/draft-calhoun-diameter-17.txt and http://www.diameter.org/; September 2000

Calhoun, Pat et al; DIAMETER Mobile IP Extensions; http://www.ietf.org/internet-drafts/draft-calhoun-diameter-mobileip-11.txt; September 2000

Calhoun, Pat et al; Mobile IP Network Access Identifier Extension for IPv4; RFC2794; http://www.ietf.org/rfc/rfc2002.txt; March 2000

Corson S. et al; Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations; RFC2501; http://www.ietf.org/rfc/rfc2501.txt; January 1999

Harkins, D. et al: The Internet Key Exchange (IKE); RFC2409; http://www.ietf.org/rfc/rfc2409.txt; November 1998

Kent, S. et al: Security Architecture for the Internet Protocol; RFC2401; http://www.ietf.org/rfc/rfc2401.txt; November 1998

Kent, S. et al; IP Encapsulating Security Payload (ESP); RFC2406; http://www.ietf.org/rfc/rfc2406.txt; November 1998

Kent, S. et al; IP Authentication Header; RFC2402; http://www.ietf.org/rfc/rfc2402.txt; November 1998

Knight, S et al; Virtual Router Redundancy Protocol; RFC2338; ftp://ftp.isi.edu/in-notes/rfc2338.txt; April 1998

Montenegro, G.; Reverse Tunneling for Mobile IP; RFC2344; http://www.ietf.org/rfc/rfc2344.txt; May 1998

Perkins, Charlie; IP Mobility Support; RFC2002; http://www.ietf.org/rfc/rfc2002.txt; October 1996

Perkins, Charlie et al; Ad hoc On-demand Distance Vector (AODV) Routing; http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-06.txt; July 2000

SUMMARY OF INVENTION

The present invention describes a network-based mobile workgroup system allowing a selected set of users from two or more mobile virtual private networks to form an extranet workgroup in a secure manner.

FIG. **2** shows the tunnel structure that is established in order to allow two mobile nodes **3***a* and **3***b* to be part of the same extranet workgroup in a secure manner. The mobile

nodes **3***a* and **3***b* are belonging to an extranet workgroup. They retrieve a list of workgroup members **26** by doing HTTPS requests **22***a* and **22***b* to the mobile service manager **7** and its portal. For each workgroup participant a triplet including the user fully qualified domain name **155***b*/**155***a*, the mobile node **3** private IP address (10.0.0.1) and the virtual home agent's **1***a*/**1***b* public IP address (204.8.9.1 and 204.8.8.1 respectively). The triplets are retrieved at sign-on to the extranet workgroup and can be updated regularly through a push or pull procedure from the mobile service manager **7** portal.

The initiating party (mobile node **3***a*) establishes a unidirectional IPSec tunnel **43***a* with the virtual home agent **1***b* for traffic going towards the mobile virtual private network that is hosted by **1***b*. Similarly the target party (mobile node **3***b*) establishes a unidirectional IPSec tunnel **43***b* with the home agent **1***a* for traffic going towards the mobile virtual private network that is hosted by **1***a*. These tunnels are encapsulated by a mobile IP tunnel **53***a*/**53***b* established from the shared foreign agent **2***a* and the individual virtual home agents **1***a* and **1***b* of each mobile virtual private network. Finally an IP—IP tunnel **53***c* is established between the two virtual home agents **1***a* and **1***b* as part of the extranet workgroup configuration from the mobile service manager **7**.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features, and advantages of the invention will be apparent from the following description of preferred example embodiments as well as illustrated in the accompanying drawings in which reference characters refer to the same parts throughout. While individual functional blocks and components are shown in many of the figures, those skilled in the art will appreciate these functions may be performed by software modules or programs executed using a suitably programmed digital microprocessor or general purpose computer by individual hardware circuits, by an application specific integrated circuit (ASIC), and/or by one or more digital signaling processors (DSPs).

FIG. **1** is a function block diagram illustrating the components in a network-based mobile virtual private network.

FIG. **2** is a function block diagram illustrating tunnel structure applied to support extranet workgroups in a network-based mobile virtual private network.

FIG. **3** is a flow chart diagram illustrating the payload header of packets sent between the foreign agent and the home agent in order to support extranet workgroups in a network-based mobile virtual private network.

FIG. **4***a* is a flow chart diagram illustrating registration message flow in order to support extranet workgroups in a network-based mobile virtual private network.

FIG. **4***b* is a flow chart diagram illustrating the data sending message flow in order to support extranet workgroups in a network-based mobile virtual private network.

FIG. **5** is a function block diagram illustrating the components of a home agent system in a network-based mobile virtual private network.

FIG. **6***a* is a flow chart diagram illustrating the internal message flow in the virtual home agent that is hosting the mobile node, which in turn request extranet access.

FIG. **6***b* is a flow chart diagram illustrating the internal message flow in the virtual home agent that is hosting the corresponding node, which a mobile node request extranet access to.

FIG. **7** is a diagram illustrating the virtual router dispatcher in a network-based home agent.

FIG. **8** is a diagram illustrating the tunnel structure used to support extranet workgroups in case of mobile nodes using co-located care of address and home agents being placed at the customer premises.

FIG. **9** is a function block diagram illustrating the components in a campus network applying mobility routing internally to track mobile nodes.

FIG. **10***a* is a function block diagram illustrating the principle of route propagation in the mobility routing protocol.

FIG. **10***b* is a flow chart diagram illustrating an extension to the Ad-hoc On-demand Distance Vector (AODV) protocol for fast handover.

FIG. **10***c* is a function block diagram illustrating the format of the AODV authentication header extension.

FIG. **10***d* is a function block diagram illustrating the format of the AODV authentication header extension when applying cryptographic authentication.

FIG. **11** is a function block diagram illustrating the support of intranet workgroups in a campus network.

FIG. **12***a* is a function block diagram illustrating the support of extranet workgroups where the mobile nodes are at their home campus networks.

FIG. **12***b* is a function block diagram illustrating the support of extranet workgroups where the mobile nodes are in visiting campus networks.

DETAILED DESCRIPTION OF THE DRAWINGS

In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular embodiments, circuits, signal formats, techniques, etc. in order to provide a thorough understanding of the present invention. Although specific protocols are referred to for purposes of facilitating the description, the present invention is not necessarily limited to such specific protocols. However, it will be apparent to one skilled in the art that the present invention may be practiced in other embodiments that depart from these specific details. In other instances, detailed descriptions of well-known methods, devices, and circuits are omitted so as not to obscure the description of the present invention with unnecessary detail.

The present invention describes a network-based mobile workgroup system allowing a selected set of users from two or more mobile virtual private networks to form an extranet workgroup in a secure manner.

The invention is based on the limited private address scenario, which entails the following:

- Mobile nodes have private addresses as defined in RFC 1918;
- Mobile nodes, having overlapping addresses may visit the same foreign agent;
- Mobile nodes support reverse tunneling;
- Each (virtual) home agent has a public IP address;
- Each (virtual) home agent is dedicated to one mobile virtual private network (M-VPN);
- Shared foreign agents have public IP addresses;
- Dedicated foreign agents may have IP addresses from the particular M-VPN realm;
- A mobile service manager has a public IP address; and
- A mobile node has a UFQDN (user fully qualified domain name) within the operator domain.

The main benefits, compared to existing solution for extranet workgroup creation, can be summarized as:

- Extranet support despite overlapping address realms;
- Flexible workgroup creation with any set of users from any set of M-VPNs;

- Supports peer-to-peer M-VPN applications between mobile clients;
- Per packet authentication and filtering by ingress M-VPN security gateway; and
- Delegated responsibility to each M-VPN to allocate resources to extranet workgroup.

FIG. **1** illustrates the placement of the home agent **1** in the operator network. The operator can either be a cellular operator with its own access network **9** or an Internet Service Provider acting as a virtual operator with no own access network **9**. In the case of a cellular operator, a foreign agent **2***a* will be shared for all mobile virtual private network customers. The foreign agent **2***a* may host multiple visited network segments **8***a* and **8***b* to which any number of mobile nodes **3***a* and **3***b* may attach. Yet again, it is important to note that the mobile nodes **3***a* and **3***b* may belong to different companies and, therefore, different mobile virtual private networks.

The home agent **1** consists of one or more virtual home agents **1***a*, **1***b*, etc. Each virtual home agent has all the components of a physical home agent. A virtual router dispatcher **11** is placed in front of the virtual home agents **1***a* and **1***b*, in order to distribute datagrams internally in the home agent **1** based on destination IP address. Each virtual home agent **1***a* and **1***b* has a public IP address for this purpose. Each virtual home agent **1***a* and **1***b* has a physical or virtual home network. This is exemplified by the physical home network **12***a* associated with the virtual home agent **1***a*.

The home agent **1** also contains a backbone virtual router **5***c* that act as the common gateway towards the Internet **6** for all virtual home agents **1***a* and **1***b*. The backbone virtual home agent **5***c* also hosts a management network **10** to which a mobile service manager **7** for the mobile workgroup system is attached. The mobile service manager **7** contains among other things a portal for workgroup membership list retrieval. The workgroup membership list is used in this invention to handle communication between workgroup memhers belonging to different address realms (mobile virtual private networks). However, it has also a more general appeal as a member list for creating any type of conference calls within the workgroup (e.g. by using Microsoft Netmeeting).

The home agent **1** is, furthermore, connected via the Internet **6** to the Intranet **6***c* and **6***d* of each company that have outsourced its mobile virtual private network. The operator has placed a foreign agent **2***c* and **2***d* at each corporate site in order to allow access to the mobile workgroup system from the Intranets **6***c* and **6***d*. Moreover, the foreign agents **2***c* and **2***d* provide independent visited networks **8***c* and **8***d* at each site at which any mobile node **3***c* and **3***d* within the mobile workgroup system can attach. This means that a mobile node **3***c* from one Intranet **6***c* can visit the corporate site of another Intranet **6***d*, if the two companies are part of a common mobile workgroup system. Note that the visited networks **8***c* and **8***d* may very well be implemented as logical networks (e.g. virtual local area networks, VLAN, or IP IP tunnels) in the existing physical infrastructure of the Intranets **6***c* and **6***d* respectively. This eliminates costly new cabling at the site and increases the reach of the visited networks **8***c* and **8***d* in the campus.

FIG. **2** shows the tunnel structure that is established in order to allow two mobile nodes **3***a* and **3***b* to be part of the same extranet workgroup in a secure manner. Note that hoth mobile node **3***a* and **3***b* are given the IP address 10.0.0.1 as their mobile virtual private networks have overlapping address realms. The foreign agent **2***a* is given a puhlic IP address 204.68.9.2 as is the two virtual home agents **1***a* and **1***b*. Virtual home agent **1***a* has IP address 204.8.9.1 and virtual home agent **1***b* has IP address 204.8.8.1. Equally important is that the mobile service manager **7** is given a public IP address 204.8.7.1 that is unique across both mobile virtual private network realms.

The mobile nodes **3***a* and **3***b* that are belonging to an extranet workgroup retrieve a list of workgroup members **26** by doing HTTPS requests **22***a* and **22***b* to the mobile service manager **7** and its portal. For each workgroup participant a triplet including the user fully qualified domain name **155***b*/**155***a*, the mobile node **3** private IP address **156***a*/*b* (10.0.0.1) and the virtual home agent's **1***a*/**1***b* public IP address **157***a*/*b* (204.8.9.1 and 204.8.8.1 respectively). The triplets are retrieved at sign-on to the extranet workgroup and can be updated regularly through a push or pull procedure from the mohile service manager **7** portal. A network address port translator **35** in the backbone virtual router **5***c* allows for the traversal of the HTTPS requests **22***a* and **22***b* from the mobile nodes **3***a* and **3***b* to the mobile service manager **7**.

The initiating party (mobile node **3***a*) establishes a unidirectional IPSec tunnel **43***a* with the virtual home agent **1***b* for traffic going towards the mobile virtual private network that is hosted by **1***b*. Similarly the target party (mobile node **3***b*) establishes a unidirectional IPSec tunnel **43***b* with the home agent **1***a* for traffic going towards the mobile virtual private network that is hosted by **1***a*. These tunnels are encapsulated by a mobile IP tunnel **53***a*/**53***b* established from the shared foreign agent **2***a* and the individual virtual home agents **1***a* and **1***b* of each mobile virtual private network. Finally an IP—IP tunnel **53***c* is established between the two virtual home agents **1***a* and **1***b* as part of the extranet workgroup configuration from the mobile service manager **7**.

FIG. **3** shows the header format of payload datagrams that are sent between the foreign agent **2***a* and the home agent **1** across the access network **9**. The top part shows the header of datagrams sent from the mobile node **3***a* and the bottom part shows the header of datagrams sent to the mobile node **3***b*. The number **40***x* denotes a destination IP address, while the number **41***x* denotes source IP address. Xa denotes the outer header, Xb the intermediate header, and Xc the inner IP header. An IPSec header **43** is placed in between the intermediate Xb and inner Xc IP header. The IPSec header **43** can either have the format of an authentication header (AH) **45** or the format of an encryption security payload (ESP) header **44** depending on security policy. Note especially that the intermediate header Xb involves the stable IP address of the mobile node **3***a*, which ensures that no renegotiation of the security association with the virtual home agent **1***b* of the other mobile virtual private network is required only because the mobile node **3***a* is changing subnetwork during the session with mobile node **3***b*.

FIG. **4***a* illustrates the registration procedure message flow when creating an extranet workgroup in a network-based mobile workgroup system, i.e. a workgroup with participants from more than one mobile virtual private network. The virtual home agents **1***a* and **1***b* are using the lightweight directory access protocol (LDAP) **25** to retrieve the extranet workgroup configurations. The virtual home agent **1***a* sends an LDAP request **25***a* to the mobile service manager **7**. The mobile service manager **7** replies with an LDAP answer **25***b* including any static routes **63** and filter states **64** to be applied to the workgroup traffic. In this particular example, the static route **63** points to the virtual home agent **1***b* of the other mobile virtual private network having members involved in the extranet workgroup. The

filter states **64** are given for each member of the workgroup **3***a* and **3***b*. In the case of workgroup members not part of the own mobile virtual private network, a realm-indexed is also supplied. In the case of mobile node **3***b*, this realm-index is the virtual home agent **1***b*, i.e. the home agent of the mobile virtual private network to which mobile node **3***b* belongs. Virtual home agent **1***b* is then configured in a similar manner using LDAP request **25***c* and answer is **25***d*.

The mobile nodes **3***a* and **3***b* within the extranet workgroup asks for the workgroup member list **26** as part of a HTTPS request **22***a*/**22***b*. The mobile service manager **7** responds with giving the triplets (the user fully qualified domain name **155** and private IP address **156** of the mobile node **3** as well as its virtual home agent **1** public IP address **157**) for each workgroup member. This means that mobile node **3***a* receives the triplets for mobile node **3***b* and vice versa.

As in the normal mobile IP registration procedure, the mobile node **3***a* sends a registration request **46***a* with only its MAC address **51***a* as source and its virtual home agent **1***a* as destination to the foreign agent **2***a*. The foreign agent **2***a* forwards the registration request **46***b* further to the virtual home agent **1***a*. The registration reply **47***a* is sent from the virtual home agent **1***a* to the foreign agent **2***a* and forwarded to the mobile node **3***a* in the form of registration reply **47***b*. The next sequence shows the corresponding procedure for mobile node **3***b*. Note that both mobile nodes are capable of using the same foreign agent **2***a*.

The initiating party (mobile node **3***a*) has now all the information and tunnel configuration information for initializing a security association with the virtual home agent **1***b* acting as security gateway for the mobile virtual private network in which the target party (mobile node **3***b*) is situated. This is performed using the Internet Key Exchange (IKE) protocol **48**. In FIG. **4***a* it is assumed that the mobile node **3***a* and the virtual home agent **1***b* has been configured with their own certificates **154***a* and **154***b* respectively. This opens up for exchanging the certificates by piggybacking them in the IKE **48** packet **5** and **9** respectively. Similarly the certificate **154***c* for the target party (mobile node **3***b*) is sent as part of IKE **48** to the security gateway of the initiating party's (mobile node **3***a*) mobile virtual private network (virtual home agent **1***a*) and vice versa. The certificates of the mobile nodes **3***a* and **3***b* are extended compared to the basic X.509v3 certificate by adding their virtual home agent's public IP address (**1***a* and **1***b* respectively) as part of the Subject Alternative Name field. This is done in order for creating a unique identity for the security association (mobile node private IP address and security gateway public IP address) that can be matched by the incoming IP—IP encapsulated IPSec datagrams. How this works will be explained in more details in FIGS. **6***a* and **6***b*.

FIG. **4***b* illustrates the message flow for sending a datagram from the mobile node **3***a* to the mobile node **3***b* and back. More specifically, it shows the source and destination IP address of each header of the packet starting with the inner packet header at the leftmost position.

FIG. **5** is the function block diagram of the home agent **1** and its individual components. The virtual router dispatcher **11** and the backbone virtual router **5***c* are shown as border components in the virtual home agent **1**. The left column shows the individual components of the virtual home agent **1***a* and the right column shows the corresponding components of the virtual home agent **1***b*. The buffer **60***a/b/c/d* is placed at the entry point of the virtual home agent **1***a*/**1***b*. An incoming datagram is stored in total in the buffer including all its IP header information. As shown by the arrows, two of the other blocks (IPSec **43***a/b* as well as the firewall **52***a/b*) are using the buffer **60***c* and **60***d* to fetch a realm-index (the virtual home agent IP address **1***b*/**1***a*). As shown in FIGS. **6***a* and **6***b*, the virtual home agent IP address **1***b*/**1***a* is always part of the datagram entering a virtual home agent from another mobile virtual private network in the form of a source IP address in an IP—IP tunnel between the two virtual home agents **1***a* and **1***b*. **50***c* and **50***d* are the two termination modules for this IP—IP tunnel. An additional set of IP—IP tunnel terminations **50***a/b* are shown at the upper part of the stack fronting the virtual router dispatcher **11** (and the foreign agent **2***a*—not shown in the picture). These IP—IP tunnel terminations relates to mobile IP.

The center module of a virtual home agent **1***a/b* is the virtual router **5***a/b*. The virtual router is making nexthop decisions for datagrams passing through the virtual home agent **1***a/b*. It is realm-specific to the mobile virtual private network that the virtual home agent **1***a/b* belongs to, and in such away can only route packets that either has public destination IP addresses or private IP addresses that belong to the address realm of its mobile virtual private network.

FIG. **6***a* is a flow chart diagram illustrating the internal message flow in virtual home agent **1***a* when a datagram arrives at the buffer **60***a* facing the foreign agent **2***a*. This is exemplified in the sequence diagram by having the initiating party (mobile node **3***a*) send a datagram towards the target party (mobile node **3***b*). The buffer **60***a* will store the whole datagram. The datagram will then be sent to the mobile IP IP—IP tunnel termination **50***a* where one header is stripped off. The datagram proceeds to the virtual router **5***a*. The virtual router **5***a* takes a forwarding decision based on the destination IP address in the datagram header, in this case the public IP address of the virtual home agent **1***b*. The forwarding table in the virtual router **5***a* has a route for **1***a* with nexthop being the logical IP—IP interface **50***c*. The datagram is, therefore, sent out on this interface, which adds a new header to the datagram with source IP address as virtual home agent **1***a* and destination address as virtual home agent **1***b*.

The lower part of the sequence diagram shows the activities performed in the virtual home agent **1***a* when a datagram is coming in on the buffer **60***c* facing the virtual home agent **1***b*. This is exemplified in the sequence diagram by having the target party (mobile node **3***b*) send a datagram towards the initiating party (mobile node **3***a*). Here again, the buffer **60***c* will store the whole datagram and send it to the logical IP—IP interface **50***c*. The IP—IP termination **50***c* will strip off the outer IP header and discover that the inner header requires IPSec decryption. The datagram is, therefore, sent to the IPSec module **43***a*. As the source header (mobile node **3***b*) is not unique (private IP address from another address realm), there is a need for the IPSec module **43***a* to query **61** the buffer **60***c* for the source address of the original incoming datagram. The reply message **62** will include the public address of the virtual home agent **1***b* (i.e. the security gateway of mobile node **3***b*). Note that in an actual implementation, sharing information from the buffer **60***c* to the IPSec module **43***a* may be solved by a common data structure. In any way, the tuplet mobile node **3***b* private IP address and virtual home agent **1***b* public IP address) will now uniquely match with the security association established using the mobile node **3***b* certificate and the initial IKE procedures **48**. The datagram can be decrypted and sent to the virtual router **5***a* for route lookup based on the destination IP address. In this case the destination IP address is mobile node **3***a*, which happens to be private but part of the address realm for which the virtual router **5***a* is allocated.

The virtual router **5***a* can in other words make a correct forwarding decision and the nexthop is the logical IP—IP interface **50***a* for mobile IP encapsulation. However, before that can be performed some security procedures will need to be performed. The reason for this is that datagram is now entering into the mobile virtual private network of virtual home agent **1***a*, and as such has to be filtered by the firewall **52***a*. In the same way as the IPsec module **43***a* could not uniquely apply filtering merely on the source IP address of mobile node **3***b*, this also applies to the firewall **52***a*. The firewall **52***a* will, therefore, query **61** the buffer **60***c* for the outer source IP address of the original incoming datagram (in this case the virtual home agent **1***b* public IP address) and apply it as realm-index in the workgroup filter. The datagram will pass the firewall **52***a* as the mobile node **3***a* is from the M-VPN, that is hosted by the security gateway **1***b*, and in addition is part of the extranet workgroup in which the destination IP address (mobile node **3***a*) is also a member in. The datagram is now sent to the logical IP—IP interface **50***a* for mobile IP encapsulation and sent towards the foreign agent **2***a*.

FIG. **6***b* describes the exact same behavior in the virtual home agent **1***b* with the mere difference that IPSec decryption **43***b* and firewall-filtering **52***b* is performed on the datagram sent from the initiating party (mobile node **3***a*) to the target party (mobile node **3***b*) instead. As the sequence diagram and numbering is similar to FIG. **6***a*, it is not described again.

FIG. **7** is a function block diagram illustrating the internal of the home agent **1** in regards to the virtual router dispatcher **11**. The virtual router dispatcher is hosted by the interface **72** facing the shared foreign agent **2***a*. Incoming packets are tunneled using mobile IP with destination address set to one of the virtual home agents **1***a* (204.8.9.1) or **1***b* (204.8.8.1). These addresses are public and, therefore unique, across all M-VPN address realms. The virtual router dispatcher can, therefore, use the destination IP address of the datagram to forward the datagram to the correct virtual home agent **1***a* or **1***b* across the internal home agent network **70**. In fact the virtual router dispatcher **11** does not only work with mobile IP tunneled datagrams, but can also be applied to any incoming datagram with a public IP address. Those datagrams with a destination IP address not matching a virtual home agent **1***a* or **1***b*, are then sent to the backbone virtual router **5***c* for further forwarding out on the Internet **6**.

One aspect in FIG. **7** is the overlapping private IP addresses of the mobile nodes **3***a* (10.0.0.1) and **3***b* (10.0.0.1). This comes from the fact that they belong to different M-VPNs and, therefore, different address realms. As can be seen from the FIG. **7**, foreign agent **2***a* has a publicly routable IP address (204.68.9.2). The datagrams, sent from anyone of the virtual home agents **1***a* or **1***b*, will be encapsulated using the foreign agent **2***a* IP address (204.68.9.2) as destination and the virtual home agent IP address as source (i.e. 204.8.9.1 for mobile node **3***a* and 204.8.8.1 for mobile node **3***b*). It is the foreign agent **2***a* that will distinguish which datagrams that shall be sent to mobile node **3***a* and **3***b* respectively. This is based on mapping the private mobile node address and public virtual home agent IP address to the unique link layer MAC address. The distribution across the visited network **8***a* and **8***b* will be based on the MAC address of the mobile node (i.e. **51***a* for mobile node **3***a* and **51***b* for mobile node **3***b*).

The description so far has been based on having the home agent **1** placed in the operator-domain, and hosting a number of virtual home agents exemplified by **1***a* and **1***b*. There are clearly some advantageous of such a network deployment scenario, where the most notable is optimal routing between mobile nodes **1***a* and **1***b* in case both are within the operator's access network **9**. In FIG. **8** it is described how extranet workgroups can be supported also in the case of having the home agents **1***a* and **1***b* physical rather than virtual and deployed at the enterprise network border rather than in the operator's core network. There are several advantageous with such a design as well, where the two most important are simplicity in home agent design and complete enterprise control of M-VPN security instead than having the control outsourced to an operator. These arguments are mostly applicable for larger campus networks. Roaming into these types of networks is, therefore, described in more detail in the next set of figures.

FIG. **8** combines the campus-based home agent **1***a* and **1***b* with the notion of co-located care-of address on the mobile nodes **3***a* and **3***b*. The co-located care-of address is an option in the mobile IP standard, and applied in case the visited network **8***a* and **8***b* does not have a foreign agent **2***a* available. In this case only a router **5***d* is available on the visited subnetworks **8***a* and **8***b*. The co-located care-of address is a last resort option and has several disadvantages compared to having a foreign agent **2***a* present. The two most important aspects relate to having two extra tunnel headers IPsec **43***c* and MIP **53***a* all the way out to the mobile node **3***a* as well as using up a public IP address as a care-of address for every mobile node. Nevertheless, the co-located care-of address is an important option to achieve widespread coverage for the extranet workgroup service. Also, using header compression schemes, like the IP header compression as defined in RFC 2507, can reduce some of the extra overhead induced by co-located care-of address on the access link towards the mobile node **3***a*.

In the campus-based home agent design, the Intranets **6***a* and **6***b* can safely be defined as home networks **12***a* and **12***b*. Instead of having an internal IP IP tunnel between two virtual home agents inside an operator-placed home agent **1**, an IP—IP tunnel **53***c* traversing the Internet **6** is established between the two home agents **1***a* and **1***b* that have mobile nodes **3***a* and **3***b* being part of the extranet workgroup. Note that an IPSec tunnel could very well replace the IP—IP tunnel **53***c*. But that it is technically not required in this particular scenario as there is always an inner IPSec security association between the sending mobile node, e.g. mobile node **3***a*, and the security gateway of the receiving M-VPN, in this case home agent **1***b*.

There are several different alternatives for securing the co-located care-of address scenario.

One alternative is to apply IPSec directly on the mobile IP tunnel **53***a* with the temporary co-located care-of address and the home agent IP address as endpoints. This requires, however, a new IKE **48** exchange at each handover as the co-located care-of address then is changing.

Another alternative is to rely on link layer security. However, this requires the placement of the home agent **1** with link layer contact to the visited subnetwork **8***a* if complete end-to-end security shall be fulfilled.

The third alternative is to apply an end-to-end IPSec security association between mobile nodes **3***a* and **3***b*. However, this prevents the home agents **1***a* and **1***b* from performing any workgroup filtering based on other aspects than mobile node IP address as all other information is encrypted (e.g. protocol type, TCP/UDP port number, etc).

The last, and selected, alternative is shown in FIG. **8** and involves adding an extra IPSec security association between the stable home address of the mobile node **3***a* and the home agent IP address **1***a*. Both are in the same M-VPN address

realm, so this causes no problem. It creates, however, some extra overhead on the access link. Overall, though, it is considered the best solution. Note also that any solution for traversing mobile IP **53***a* through a network address port translator (NAPT) will automatically also solve the problem of traversing the IPSec tunnel **43***c* across the same NAPT.

As pointed out in the description of current state of the art, a mobility-aware, and security conscious, network-layer is the obvious missing piece for campus-wide mobility to be a reality. This missing piece can either be implemented using mobile IP, mobility routing or a combination of the two. The following invention applies a combination of the two, i.e. mobility routing is applied as the intra-domain routing protocol and mobile IP as the inter-domain routing protocol. The reason being that mobile IP is applying a tunneling technique that has scalability characteristics already well-proved in other wide-area mobile systems, but introduces a complexity of tunnel management not suitable for dense campus networks. Mobility routing, with its flat topology and reactive routing scheme, has on the other hand the flexibility required for the adhoc mobility behavior one can expect in a campus area. Furthermore, the following invention suggests a proactive route update extension for active sessions in order to provide the foundation for a fast handover procedure necessary for real-time critical applications such as voice of IP.

FIG. **9** is a function block diagram illustrating a large campus network. In a complete installation, all nodes in the distribution layer **38** of a large campus network will be equipped with mobility routing **31**, while only the inner firewall routers **31*** of the WAN distribution layer **36** will be equipped with additional mobile IP functionality. Multiple equal cost paths may be available between two mobility routers **31**, in which case the mobility routing protocol will perform load balancing between the two paths. Obviously, a company may merely install a firewall router **31*** and no other distribution nodes **31** at a smaller branch office. Furthermore, an enterprise may decide to introduce mobility routing **31** gradually into the campus network, e.g. by restricting the deployment to the segments where Wireless LAN access points **33** are deployed at the access layer **39**. The mobility routers **31** will be able to function in such a mixed campus environment as well, by running traditional intra-domain routing protocols, like OSPF. The OSPF protocol then has dual purposes. It is partly used to create tunnels between mobility routing nodes **31** for the purpose of carrying mobility routing traffic, and it is partly used to publish aggregate routes for the mobile nodes **3** towards the core layer **37** switches **32**/routers **5** and the remaining part of the distribution layer **38** routers **5**.

Both the WAN distribution layer **36** and the server farm **80** contain servers **34**. The servers **34** hosted by the WAN distribution layer **36** are normally accessible from both the Internet **6** (via router **5***) and from the Intranet **6***c*. The servers **34** hosted by the server farm **80** are, on the other hand, only accessible from within the Intranet **6***c*.

The mobile service manager (MSM) **7** for a company will typically be placed at the WAN distribution layer **36** in order to be accessible from the inside as well as from the outside. From a network perspective it will function as a centralized data store from which the mobility routers **31** can fetch user and workgroup profiles. From a management viewpoint, it will be the portal to which the IT-administrator and workgroup members login for managing profiles and exchanging service information.

FIG. **10***a* illustrates how route propagation is performed within the campus network (also described as Intranet **6***c* and home network **12** in this invention). The mobility routing protocol is based on a reactive **55** protocol, like the Ad-hoc On-demand Distance Vector (AODV) protocol as defined in the IETF. In such a protocol, no peers **3***d*, **3***e*, or **3***f* are automatically updated with a new route to mobile node **3***a* and its (personal area network **54**) as it moves from mobility router **31***f* to mobility route **31***a*. Similarly, no mobility routers (**31***a*, **31***d*, **31***e* and **31***f*) are updated with the new route unless someone requests them for it. The benefit of this is that the load of route updates becomes low compared to complete proactive routing. Especially in the case when mobile nodes are moving a lot and they are not communicating with too many peers at the same time. This is typically the case in an Intranet **6***c*, which has applied a mobile virtual private network across multiple sites. A mobile node **3***a* will then normally communicate with only a few active peers **3***b* and **3***c* at the local site as well as some active peers **3***d* at the headquarters of the company. The mobile node **3***a* will rarely communicate with other local sites such as the inactive peer **3***e*.

The following invention extends the basic principle of reactive routing as defined in AODV, in order to preserve the reactive **55** nature of the protocol updates to inactive peers **3***f* and **3***e*, while implement a proactive **56** routing update to active peer **3***d* and its mobility router **31***d*. This extension ensures a high speed, and equally importantly low packet loss, at handovers. Thus, this mobility routing protocol is using a combination of proactive **56** and reactive **55** route propagation in order to maintain a flat route topology (stable IP addresses for all mobile nodes **3**). Proactive advertisements **56** are only propagated to active peers **3***d* (on-going sessions), while inactive peers **3***e* and **3***f* will request a route to the mobile node **3***a* (and its personal area network **54**) only if initiating a session. FIG. **10***b* illustrates in more details the proactive route advertisements that are added to a reactive routing protocol like Ad-hoc On-demand Distance Vector (AODV) in order to create a fast handover of a mobile node **3***a* from one mobility router **31***f* to another mobility router **31***a*.

The mobile node **3***a* sends a hello message to its new sink (mobility router **31***a*) with a destination sequence number **111** set to equal to the last registration reply distributed via the old sink (mobility router **31***f*). The mobility router **31***a* takes this first registration reply as a hello message and an indication that it now is asked to take the role of new sink in the core mobility router network for mobile node **3***a*. If it has already an existing route towards mobile node **3***a*, with same destination sequence number **111** as received in the hello message, it can start directly to send an unsolicited route reply in the direction towards the old sink (mobility router **31***f*. If it does not have a route already towards mobile node **3***a*, it discovers it by sending a route request with the destination sequence number **111** as received from mobile node **3***a* in the hello message. The earlier sink (mobility router **31***f*), or any mobility router along the path, will then respond with a route reply message. This is then followed by an unsolicited route reply from the new sink (mobility router **31***a*) along the same path and having the destination sequence number **111** incremented by one. The old sink (mobility router **31***f*) and all mobility routers along the path between the old and the new sink are updated with the new route having a better destination sequence number **111**+1. The old sink (mobility router **31***f*) now will forward all datagrams destined to mobile node **3***a* via the mobility router **31***a*. A route reply is sent to the mobile node **3***a* indicating that the handover procedure was successful. The mobile

node **3***a* may now smoothly migrate from the old (mobility router **31***f*) to the new link (mobility router **31***a*).

The mobile node **3***a* may at its leisure also decide to optimize the path towards active peer (mobile node **3***d*), by initiating route requests towards this destination. The source sequence number (SSN) **112** in these messages are set equal to the new destination sequence number (DSN) **111**+1 for mobile node **3***a*. Bi-directional, optimal paths are now established.

The handover procedure for AODV as defined in FIG. **10***b* is also suitable for protecting the mobile node **3***a* against access point **33**, access link and mobility router **31** failure. As shown in FIG. **9**, the access point **33** normally is only equipped with one interface uplinks towards the distribution layer **38** mobility router **31**. In fixed IP networks this constitute a single point of failure at the physical layer and is not recommended. However, in a wireless access layer **39** equipped with a flat mobility routing **31** distribution layer **38**, the route update sequence for handover can be applied also at access point **33**, access link or old mobility router **31** sink failure. The only difference compared to the handover procedure as described above, is that the new sink (mobility router **31***a*) will not receive any route reply from a malfunctioning old sink (mobility router **31***f*). The new sink (mobility router **31***a*) will, therefore, send a route error rather than a route reply back to the mobile node **3***a*. The mobile node **3***a* will take this as an indication that no forwarding path has been created from the old sink (mobility router **31***f*) to the new sink (mobility router **31***a*) and immediately start sending route requests towards the active peer (mobile node **3***d*) in order to repair the path for ongoing sessions.

Furthermore, it shall be noted that the AODV implementation in the mobile node **3***a*, and as depicted in FIG. **10***b*, also can be implemented as a proxy in the ingress mobile service router **31***a*. This eliminates the requirement on AODV implementation on the mobile node **3***a*. The mobile node **3***a* will instead utilize a Dynamic Host Configuration Protocol (DHCP) request as its hello message to a new sink **31***a*. The DHCP request will include the stable IP address of the mobile node **3***a* and an authenticator for the sink to send further up to the mobile service manager **7** (see FIG. **10***c* for more explanation on how an authenticator is utilized in the mobile workgroup system). The new sink **31***a* will then act as a proxy for the mobile node **3***a* and initiate the handover procedure with old sink **31***f* in the same way as described in FIG. **10***b*. For the part on optimizing routes, as shown in the lower part of FIG. **10***b*, the new sink **31***a* will initiate such route requests on behalf of the mobile node **3***a*, based on receiving a datagram from the mobile node **3***a* with the destination set to mobile node **3***d*. The reminder of the sequence diagram in FIG. **10***b* can then be kept unchanged also in the proxy case.

In AODV route requests are being broadcasted, while route replies are being sent using unicast. Broadcast route requests that are sent due to lifetime expiration of an active path are not very effective and cause unnecessary load in the network. For this reason, this invention introduces a gratuitous route reply that can be sent by a route reply source before the route lifetime has expired. Such a gratuitous route reply can be sent using unicast towards the source of the initial route request. For this purpose, a mobility router **31** can be configured with a route reply trigger that specifies the number of seconds that max will remain before a gratuitous route reply will he sent for an active route. The term active route does in this context mean a route for which the mobile service router **31**, acting as the source of the original route reply, can detect that datagrams are continuously being forwarded for. By using the gratuitous route reply procedure the mobile workgroup system will allow ongoing streaming sessions with no interruptions due to expiration of route lifetimes.

In the section above, one way to limit broadcasts in the network was described in the form of gratuitous route replies for active sessions. In order to limit the width of broadcast route requests for a new route, AODV recommend the use of expanding ring search based on hop count. This allows a crude way to stepwise search wider for a route reply on a route request for a destination. However, as described in FIG. **9**, all the mobility routers **31** at the distribution layer have IP—IP tunnels to each other and therefore all are one hop away. If applying the expanding ring search, this would mean a drastic increase in route requests at the distribution layer border. This invention applies a configurable weight instead of a 1 for each hop in the mobility routing network. With setting the weight differently for different neighbors, the distribution layer network could be segmented, e.g. geographically, so that an expanding ring search would gradually increase more and more neighbor distribution layer routers **31** in FIG. **9**.

FIG. **10***c* shows the second extension to AODV necessary to support mobile workgroups. The extension relates to authentication and FIG. **10***c* shows the header format of an AODV message applying such an extension. The AODV authentication extension is applied on route requests and replies between neighbors (mobile nodes **3** and mobility routers **31**). The extension has a similar format to the scheme as applied to OSPF in RFC 2328.

Version **71**: The AODV version number. This specification documents version **2** of the protocol.

Type **73**: The AODV packet types are as follows:

Type	Description
1	Route Request
2	Route Reply
3	Route Error
4	Route Reply Acknowledgment

Packet length **74**: The length of the AODV protocol packet in bytes. This length includes the standard AODV header.

Router ID **78**: The Router ID of the packet's source. It can be a mobility router **31** or a mobile node **3**.

Checksum **75**: The standard IP checksum of the entire contents of the packet, starting with the AODV packet header but excluding the 64-bit authentication field. This checksum is calculated as the 16-bit one's complement of the one's complement sum of all the 16-bit words in the packet, excepting the authentication field. If the packet's length is not an integral number of 16-bit words, the packet is padded with a byte of zero before checksumming. The checksum is considered to be part of the packet authentication procedure; for some authentication types the checksum calculation is omitted.

AuType **76**: Identifies the authentication procedure to be used for the packet.

Authentication **77***a* and b: A 64-bit field for use by the authentication scheme.

All AODV protocol version **2** exchanges are authenticated. The AODV packet includes an authentication type field **76**, and 64-bits of data for use by the appropriate authentication scheme (determined by the type field **76**).

The authentication type **76** is configurable on a per-interface (or equivalently, on a per-network/subnet) basis. Additional authentication data **77** is also configurable on a per-interface basis. Authentication types (**76**) **0**, **1** and **2** are defined by this specification. All other authentication types **76** are reserved for definition by the IANA (iana@ISI.EDU). The current list of authentication types **76** is described below:

AuType	Description
0	Null authentication
1	Simple password
2	Cryptographic authentication

All others are reserved for assignment by the IANA (iana@ISI.EDU)

Null authentication: Use of this authentication type **76** means that routing exchanges over the network/subnet are not authenticated. The 64-bit authentication field **77** in the AODV header can contain anything; it is not examined on packet reception. When employing Null authentication, the entire contents of each AODV packet (other than the 64-bit authentication field **77**) are checksummed in order to detect data corruption.

Simple password authentication: Using this authentication type **76**, a 64-bit field is configured on a per-network basis. All packets sent on a particular network must have this configured value in their AODV header 64-bit authentication field **77**. This essentially serves as a "clear" 64-bit password. In addition, the entire contents of each AODV packet (other than the 64-bit authentication field) are checksummed in order to detect data corruption.

Simple password authentication guards against routers (mobile node **3** or mobility router **31**) inadvertently joining the routing domain; each router must first be configured with its attached networks' passwords before it can participate in routing. However, simple password authentication is vulnerable to passive attacks. Anyone with physical access to the network can learn the password and compromise the security of the AODV routing domain.

Cryptographic authentication: Using this authentication type **76**, a shared secret key is configured in all routers attached to a common network/subnet. For each AODV protocol packet, the key is used to generate/verify a "message digest" that is appended to the end of the AODV packet. The message digest is a one-way function of the AODV protocol packet and the secret key. Since the secret key is never sent over the network in the clear, protection is provided against passive attacks.

The secret key specifies the algorithms used to generate and verify the message digest implicitly. This invention suggests an AODV cryptographic authentication by using the MD**5** algorithm. The format of the authentication field **77***a* and **77***b*, in the case of cryptographic authentication, is shown in FIG. **10***d*.

A non-decreasing sequence number is included in each AODV protocol packet to protect against replay attacks. This provides long-term protection; however, it is still possible to replay an AODV packet until the sequence number changes. To implement this feature, each neighbor data structure contains a new field target the "cryptographic sequence number" **91**. This field is initialized to zero, and is also set to zero whenever the neighbor's state transitions to "Down". Whenever an AODV packet is accepted as authentic, the cryptographic sequence number **91** is set to the received packet's sequence number.

This invention does not provide a rollover procedure for the cryptographic sequence number **91**. When the cryptographic sequence number that the router is sending reach the maximum value, the router should reset the cryptographic sequence number **91** that it is sending back to 0. After this is done, the router's neighbors will reject the router's AODV packets for a period of the configured router dead interval, and then the router will be forced to re-establish all adjacencies over the interface. However, it is expected that many implementations will use "seconds since reboot" (or "seconds since 1960", etc.) as the cryptographic sequence number **91**. Such a choice will essentially prevent rollover, since the cryptographic sequence number field **91** is 32 bits in length.

The AODV cryptographic authentication option does not provide confidentiality.

When cryptographic authentication is used, the 64-bit authentication field **77** in the standard AODV packet header is redefined as shown in FIG. **10***d*. The new field definitions are as follows:

Key ID **79**: This field identifies the algorithm and secret key used to create the message digest appended to the OSPF packet. Key Identifiers **79** are unique per-interface (or equivalently, per-subnet).

Auth Data Length **90**: The length in bytes of the message digest appended to the AODV packet.

Cryptographic sequence number **91**: An unsigned 32-bit non-decreasing sequence number. Used to guard against replay attacks.

FIG. **11** illustrates the deployment of an Intranet workgroup across two or more sites interconnected by an IPSec tunnel **30**. The Intranet is applying mobility routing internally in the home network **12** as well as the authentication extension **27** for the mobility routing advertisements **29**. As is shown in FIG. **11**, there is a mobile service manager **7***a* deployed at one of the sites in the home network **12**. When a mobile node **3***a* sends a route request for the first time to a mobility router **31***a*, the mobility router **31***a* will send a DIAMETER request **28** to the mobile service manager **7***a* for centralized authentication and configuration download. The DIAMETER response **29** from the mobile service manager **7***a* will include static routes **63** and filters states **64** that shall be applied for traffic from/to the mobile node **3***a*. In particular a default route to the home network **12** gateway mobility router **31***c* as well as the IP address range for the home network **12** is received. These two static routes are sent further in the route reply **29** to the hello message from the mobile node **3***a*. The mobile node **3***a* now knows for which address range it shall broadcast AODV reactive **55** route requests instead of applying the default route **31***c*. Note that the default route can be reached through unicasting route requests.

A variant to the above mentioned shared key authentication procedure, is that the mobile workgroup system applies public keys and certificates for mobile node **3***a* authentication. The mobile node **3***a* will then piggyback its X.509 certificate when sending the initial hello message to a new sink **31***a*. The sink **31***a* verifies that the certificate is signed by the mobile service manager and uses the public key of the received certificate to authenticate the mobile node **3***a*. The sink then sends its certificate to the mobile node **3***a*, whereas the mobile node **3***a* verifies that the certificate is signed by the mobile service manager **7** and uses the public key of the received certificate to authenticate the mobile service router **31***a* acting as new sink. The own certificate and the mobile

service manager's **7** certificate are retrieved by the mobile node **3***a* and the mobile services router **31***a* from the mobile service manager **7** as part of management configuration. As an alternative, the mobile node **3***a* certificate may also be retrieved by the mobile services router **31***a* from the mobile service manager **7** as a domain name system query triggered by the initial hello message or as a DIAMETER query triggered by the initial hello message.

FIGS. **12***a* and **12***b* illustrate the more complex case of creating an extranet workgroup, i.e. a workgroup across two or more home networks (**12***a* and **12***b*). FIG. **12***a* illnstrates the case where the mobile nodes **3***a* and **3***b* are in their respective home networks **12***a* and **12***b*. The gateways router MR **31***c* has now also been equipped with home agent functionality **1***a*. The home agents **1***a* and **1***b* are acting as security gateways for each mobile virtual private network (in FIG. **12***a* depicted as mere bome networks **12***a* and **12***b*). As described in detail in FIGS. **4***a*/**4***b* and **6***a*/**6***b*, the initiating party (mobile node **3***a*) is establishing an IPSec security association **43***a* with the target party's (mobile node **3***b*) security gateway (home agent **1***b*). Similarly, the target party (mobile node **3***b*) is establishing an IPSec security association **43***b* with the initiating party's (mobile node **3***a*) security gateway (home agent **1***a*). Each security gateway (**1***a* and **1***b*) can now perform realm-indexed workgroup filtering on incoming packets to the home network (**12***a* and **12***b*). The extranet workgroup lilters that are used by the security gateways (**1***a* and **1***b*) are fetched from the common mobile service manager **7***c*.

There may still be local mobile service managers (**7***a* and **7***b*) that only controls Intranet workgroups. Their behavior is the same as described in FIG. **11**.

FIG. **12***b* illustrates the most complex scenario of an extranet workgroup, in which case the mobile node **3***b* is visiting inside home network **12***a* and mobile node **3***a* is visiting in home network **12***b*. When the mobile node **3***b* is trying to authenticate itself with the mobility router **31***a*, the answer from the mobile service manager **7***a* will merely be a default route to the foreign agent **2***a* (co-located with mobility router **31***c*). Only this default route is advertised to the mobile node **3***b*. The sink (mobility route **31***a*) of mobile node **3***b* will reject all datagrams with another destination than foreign agent **2***a*. It is also possible to limit the usage of the home network **12***a* even further by only allowing the IPSec **43***c* protocol through.

The foreign agent **2***a* will act with normal mobile IP behavior and establish a mobile IP tunnel **53***b* to the home agent **1***b* of mobile node **3***b*. The home agent **1***b* will look up the destination IP address of the datagram (mobile node **3***a*) in the routing table and send it further through the IP—IP tunnel **53***c* to the home agent **1***a*. Note that ipUnplugged has submitted another patent request named "A route optimization technique for mobile IP". If this is applied in the present invention, the foreign agent **2***a* will not need to send datagrams through the mobile IP tunnel **53***b* to the home agent **1***b*. Instead, the datagram can be directly routed to the home agent **1***a*.

The home agent **1***a* will perform the extranet workgroup filtering based on configuration from the common mobile service manager **7***c* and then send the packet via the mobile IP tunnel **53***a* to the foreign agent **1***b* for further distribution to the mobile node **3***a*. Datagrams that are sent in the other direction from the mobile node **3***a* to the mobile node **3***b* are treated the same way using the IPSec tnnnel **43***d* instead.

What is claimed is:

1. A mobile routing system, comprising:

a mohile node;

a plurality of sinks in a computer network, the plurality of sinks including a plurality of mobile routers; and

memory storing computer readable instructions, that, when executed by the processor, cause the routing system to perform a method that includes the steps of:

detecting movement of the mobile node between the plurality of sinks in the computer network; and

maintaining a connection by maintaining a stable IP address for the mobile node and sustaining, without packet loss, one or more active application sessions between the mobile node and one or more active peers upon detecting movement of the mobile node in accordance with a predefined reactive routing protocol, wherein the reactive routing protocol is extended by a proactive routing update for the one or more active peers upon detecting movement of the mobile node from an old sink to a new sink, and

wherein one or more replies to a route request sent from the new sink establishes a bi-directional, optimal path between the mobile node and one or more of the active peers.

2. The routing system of claim **1**, wherein the reactive routing protocol includes an Ad-boc On-Demand Distance Vector (AODV) protocol.

3. The routing system of claim **2**, wherein the mobile node transmits an initial message to the new sink with a destination sequence number set equal to a destination sequence number of a last registration reply that was distributed via the old sink.

4. The routing system of claim **3**, wherein the new sink treats the message as an indication that the mobile node is requesting the new sink to act as the mobile node's ingress router in the network.

5. The routing system of claim **4**, wherein the new sink transmits an unsolicited route reply toward the old sink if the new sink has an existing route toward the mobile node in a routing table of the new sink and if the destination sequence number is the same for the route as the one received from the mohile node in the initial message.

6. The routing system of claim **5**, wherein the new sink sends a route request with a destination sequence number set to the same value as the sequence number received from the mobile node in the initial message.

7. The routing system of claim **6**, wherein the old sink or a mohility ronter along a path to the old sink, responds with a route reply message.

8. The routing system of claim **7**, wherein the new sink sends an unsolicited route reply message for the mobile node destination with the route request source IP address set to the old sink and the destination sequence number incremented by one.

9. The routing system of claim **8**, wherein the old sink and one or more mobility routers along the path to the old sink and one or more mobility routers along a path to the new sink are updated with a new route having a preferred destination sequence number.

10. The routing system of claim **9**, wherein the old sink forwards packets destined to the mobile node along a route via the new sink.

11. The routing system of claim **10**, wherein a route reply is sent from the old sink via the new sink to the mobile node to indicate that a handover procedure has been successful and wherein the new sink sends a route error to the mobile node if it cannot reach the old sink.

12. The routing system of claim **11**, wherein the mobile node migrates a forwarding of datagrams from a link of the old sink to a link of the new sink.

13. The routing system of claim 12, wherein the mobile node determines an optimized path toward active peers by initiating route requests toward the active peers.

14. The routing system of claim 13, wherein a source sequence number in the route request to an active peer is set equal to the new destination sequence number of the mobile node.

15. The routing system of claim 1, wherein a mobile service router sink also acts as a proxy for mobility routing protocol exchanges between the mobile node and the network in that the mobile service router sink initiates a route request on behalf of the mobile node upon receipt of a datagram from the mobile node not compliant with an adhoc routing protocol applied in the computer network.

16. The ronting system of claim 15, wherein the mobile node uses a Dynamic Host Configuration Protocol (DHCP) request as an initial message to the new sink.

17. The routing system of claim 16, wherein the DHCP request includes the mobile node's IP address and authenticator.

18. The routing system of claim 17, wherein the mobile router sink maps the DHCP request to at least one of a RADIUS request or a DIAMETER request further sent to a mobile service manager for authentication.

19. The routing system of claim 18, wherein the mobile router sink initiates a route request on behalf of the mobile node upon receipt of a datagram from the mobile node.

20. The routing system of claim 19, wherein the mobile router sink buffers received datagrams until a path is established to a destination of the datagrams.

21. The routing system of claim 1, wherein a source of a route reply is configured to initiate a gratuitons route reply toward the source in order to provide continuous streaming of datagrams for active application sessions.

22. The routing system of claim 21, wherein the source of the route reply sends the gratuitous route reply if a life time of the route is expiring within a configured number of seconds and datagrams are received along a path between the mobile node and the one or more active peers.

23. A mobile routing system, comprising:

a mobile node;

a plurality of sinks in a computer network, the plurality of sinks including a plurality of mobile routers; and

memory storing computer readable instructions, that, when executed by the processor, cause the routing system to perform a method that includes the steps of:

detecting movement of the mobile node between the plurality of sinks in the computer network; and

maintaining a connection by maintaining a stable IP address for the mobile node and sustaining, without packet loss, one or more active application sessions between the mobile node and one or more active peers upon detecting movement of the mobile node in accordance with a predefined reactive routing protocol,

wherein the reactive routing protocol includes an Ad-hoc On-Demand Distance Vector (AODV) protocol,

wherein the routing system is further configured to extend the reactive protocol with a proactive routing update for the one or more active peers upon detecting movement of the mobile node from an old sink to a new sink,

wherein the mobile node transmits an initial message to the new sink with a destination sequence number set equal to a destination sequence number of a last registration reply that was distributed via the old sink,

wherein the new sink treats the message as an indication that the mobile node is requesting the new sink to act as the mobile node's ingress router in the routing system network,

wherein the new sink transmits an unsolicited route reply toward the old sink if it has an existing route toward the mobile node in a routing table of the new sink end if the destination sequence number is the same for the route as the one received from the mobile node in the initial message,

wherein the new sink sends a route request with a destination sequence number set to the same value as the sequence number received from the mobile node in the initial message,

wherein the old sink or a mobility router along a path to the old sink, responds with a route reply message,

wherein the new sink sends an unsolicited route reply message for the mobile node destination with the route request source IP address set to the old sink and the destination sequence number incremented by one,

wherein the old sink and one or more mobility routers along the path to the old sink and one or more mobility routers alone a path to the new sink are updated with a new route having a preferred destination sequence number,

wherein the old sink forwards packets destined to the mobile node along a route via the new sink,

wherein a route reply is sent from the old sink via the new sink to the mobile node to indicate that a handover procedure has been successful and wherein the new sink sends a route error to the mobile node if it cannot reach the old sink,

wherein the mobile node migrates a forwarding of datagrams from a link of the old sink to a link of the new sink,

wherein the mobile node determines an optimized path toward active peers by initiating route requests toward the active peers,

wherein a source sequence number in the route request to an active peer is set equal to the new destination sequence number of the mobile node, and

wherein one or more replies to the route request establishes a bi-directional, optimal path between the mobile node and the one or more active peers.

24. A mobile routing system, comprising:

a mobile node;

a plurality of sinks in a computer network, the plurality of sinks including a plurality of mobile routers; and

memory storing computer readable instructions, that, when executed by the processor, cause the routing system to perform a method that includes the steps of:

detecting movement of the mobile node between the plurality of sinks in the computer network; and

maintaining a connection by maintaining a stable IP address for the mobile node and sustaining, without packet loss, one or more active application sessions between the mobile node and one or more active peers upon detecting movement of the mobile node in accordance with a predefined reactive routing protocol,

wherein weights are assigned to neighbor hops in order to limit broadcast route requests when applying an expanding ring search algorithm in a reactive routing protocol.

25. The routing system of claim 24, wherein a weight for a hop can be administratively configured on a mobile router.

26. The routing system of claim 25, wherein a sum of weights from a source IP address of a request to the mobile router is used to select a path.

27. The routing system of claim 26, wherein mobile routers to which an expanding ring search route request is sent is limited to one or more mobile routers that have the lowest sum of weights from the source IP address of the request to a candidate neighbor mobile router.

28. A mobile routing system, comprising:

a mobile node;

a plurality of sinks in a computer network, the plurality of sinks including a plurality of mobile routers; and

memory storing computer readable instructions, that, when executed by the processor, cause the routing system to perform a method that includes the steps of:

detecting movement of the mobile node between the plurality of sinks in the computer network; and

maintaining a connection by maintaining a stable IP address for the mobile node and sustaining, without packet loss, one or more active application sessions between the mobile node and one or more active peers upon detecting movement of the mobile node in accordance with a predefined reactive routing protocol,

wherein a source of a route reply is configured to initiate a gratuitous route reply toward the source in order to provide continuous streaming of datagrams for active application sessions,

wherein the source of the route reply sends the gratuitous route reply if a life time of the route is expiring within a configured number of seconds and datagrams are received along a path between the mobile node and the one or more active peers, and

wherein the configured number of seconds triggering gratuitous route reply from the route reply source is larger than a configured number of seconds left on the route lifetime triggering a new route request from the route request source.

29. A mobile routing system, comprising:

a mobile node;

a plurality of sinks in a computer network, the plurality of sinks including a plurality of mobile routers; and

memory storing computer readable instructions, that, when executed by the processor, cause the routing system to perform a method that includes the steps of:

detecting movement of the mobile node between the plurality of sinks in the computer network; and

maintaining a connection by maintaining a stable IP address for the mobile node and sustaining, without packet loss, one or more active application sessions between the mobile node and one or more active peers upon detecting movement of the mobile node in accordance with a predefined reactive routing protocol,

wherein a source of a route reply is configured to initiate a gratuitous route reply toward the source in order to provide continuous streaming of datagrams for active application sessions,

wherein the source of the route reply sends the gratuitous route reply if a life time of the route is expiring within a configured number of seconds and datagrams are received along a path between the mobile node and the one or more active peers, and

wherein the gratuitous route reply is unicast along a spanning tree created for active sessions towards a destination.

* * * * *

EXHIBIT 1004
Curriculum Vitae of
Dr. Michael I. Shamos

Resume of Michael Ian Shamos

Current to May 8, 2024

Education

A.B. (1968) Princeton University (Physics). Thesis: "Gravitational Radiation Reaction." Advisor: John A. Wheeler.

M.A. (1970) Vassar College (Physics). Thesis: "An Absorber Theory of Acoustical Radiation." Advisor: Morton A. Tavel.

M.S. (1972) American University (Technology of Management).

M.S. (1973) Yale University (Computer Science).

M.Phil. (1974) Yale University (Computer Science).

Ph.D. (1978) Yale University (Computer Science). Thesis: "Computational Geometry". Thesis committee: David Dobkin, Martin H. Schultz, Stanley C. Eisenstat.

J.D. (1981) Duquesne University, *cum laude.*

Foreign Languages

French, Russian (good reading and technical translation skills, fair conversational ability).

Academic Experience

Distinguished Career Professor, Language Technologies Institute and Software and Social Systems Department, School of Computer Science, Carnegie Mellon University (2001-)
Principal Systems Scientist (1998-2001)
Principal Lecturer (2002-2003). Teaching Professor (2003-)
Faculty, Tepper School of Business, Carnegie Mellon University (1999-2004).
Co-Director, Carnegie Mellon Institute for eCommerce (1998-2004)
Vice-Chair, University Research Council (2000-2002)
Director, eBusiness Technology degree program, Carnegie Mellon (2003-2018)
Director, M.S. in Artificial Intelligence and Innovation, Carnegie Mellon (2018-)
Affiliated Faculty, CMU Center for Informed Democracy and Social-cybersecurity (2021-)
Core faculty, Privacy Engineering degree program (2013-)
Director, Universal Library, Carnegie Mellon University (1998-)
Visiting Professor, Faculty of Engineering, The University of Hong Kong (2001-2021)
Adjunct Faculty, Carnegie Mellon University, Department of Computer Science (1981-1998)

Assistant Professor, Carnegie Mellon University, Departments of Computer Science and Mathematics (1975-81), Dept. of Statistics (1978-81).

Courses taught (Carnegie Mellon):
Algorithm Design and Analysis 15-451 (Comp. Sci.)
Intellectual Capital and its Protection 45-886 (MBA)
Ecommerce Technology 20-751 (MSEC program)
Electronic Payment Systems 20-753 (MSEC program), 96-774 (MSIT program)
Ecommerce Law and Regulation 46-840 (MSEC program)
Electronic Voting 17-803
Ubiquitous Computing, 96-761 (MSIT Program)
Electronic Payment Systems (MSIT Program)
Law of Computer Technology, 17-762/17-662/17-562 (2007-)
Artificial Intelligence and Future Markets, 11-561 (2018-)

Honors and Awards

Fellow, Society of the Sigma Xi (1974-83).

IBM Fellowship, Yale University (1974–75).

SIAM National Lecturer (1977–78).

Distinguished Lecturer (computer science), University of Rochester (1978); McGill University (1979).

Duquesne University Law Review (1980–81).

Black & White Scotch Achiever's Award (first annual, 1991, for contributions to bagpipe musicography).

Industry Service Award of the Billiard and Bowling Institute of America, 1996 (for contributions to billiard history).

Billiard Worldcup Association official referee (2001-)

Editorships

Editor-in-Chief, Journal of Privacy Technology (2003- 2006).

Member of Editorial Board, *Electronic Commerce Research Journal* (2000-).

Member of Editorial Board, *Pittsburgh Journal of Technology Law and Policy* (1999-2003).

Dr. Shamos has reviewed scientific papers for *Communications of the ACM*, *Mathematical Reviews*, *IEEE Computer*, *IEEE Transactions on Computers*, *Information Processing Letters*, *Journal of the ACM* and the *Journal of Computational Physics*.

Contributing Editor, *Billiards Digest* magazine (1990-).

Patents

Co-inventor with K. Srinivasan, U.S. Patent 7,330,839, "Method and System for Dynamic Pricing," issued February 12, 2008.

Co-inventor with K. Srinivasan, U.S. Patent 7,421,278, "Method and Apparatus for Time-Aware and Location-Aware Marketing," issued September 2, 2008.

Co-inventor with K. Srinivasan, U.S. Patent 7,747,465, "Determining the Effectiveness of Internet Advertising," issued June 29, 2010.

Co-inventor with K. Srinivasan, U.S. Patent 8,195,197, "Method and Apparatus for Time-Aware and Location-Aware Marketing," issued June 5, 2012.

Co-inventor with K. Srinivasan, U.S. Patent 8,280,773, "Method and Apparatus for Internet Customer Retention," issued October 2, 2012.

Co-inventor with K. Srinivasan, U.S. Patent 9,456,299, "Method and Apparatus for Time-Aware and Location-Aware Marketing," issued September 27, 2016.

Legal Experience

Special Counsel, Reed Smith LLP (2000-2003), electronic commerce law.

Shareholder, The Webb Law Firm (1996-2000), intellectual property law. Associate (1990-95).

Private practice of law (1987-90), intellectual property

Associate, law firm of Buchanan, Ingersoll, P. C. (1985-87)(now Buchanan Ingersoll & Rooney, PC), Emerging Companies Department.

General Counsel, Carnegie Group, Inc. (1983-85), artificial intelligence company.

Private practice of law (1981-83), computer law.

Bar Admissions

Supreme Court of Pennsylvania (1981–).

United States District Court for the Western District of Pennsylvania (1981–).

United States Patent and Trademark Office (1981–).

United States Tax Court (1982–).

United States Court of Appeals for the Armed Forces (1982–).

United States Court of Appeals for the Third Circuit (1982–).

United States Supreme Court (1985–).

United States Court of Appeals for the Federal Circuit (1985–).

Expert Witness

Dr. Shamos has served as an expert witness in multiple computer software and electronic voting cases. He has participated in the cases listed below. "D" indicates deposition testimony; "R" indicates report, declaration or affidavit; "T" indicates trial testimony.

Total: 384 cases, including 302 patent, 20 electronic voting, 21 trade secret, 13 copyright, 1 criminal.
Affidavits, reports or declarations submitted in 271 cases.
Deposed in 158 cases.
Testified at trial or hearing in 50 cases (20 jury trials).
Participated in 7 ITC investigations, 121 IPRs, 22 CBMs, 10 PGRs, and 4 reexams.

1. *C.W. Communications, Inc. v. International Research Service, Inc.*, Civil Action No. 84-890, (W.D. Pa. 1984), aff'd. Case No. 88-3331 (3d Cir., Oct. 31, 1988). Served as an expert for plaintiff publisher as to the fame of its "Computerworld" trademark. Result: permanent injunction entered against defendant. Judge McCune's Memorandum and Order states. "We accept the conclusion drawn by Dr. Shamos." Firm: Webb, Burden Robinson & Webb (now the Webb Law Firm). (D,T)

2. *E.F. Hutton, Inc. v. Gipson* (W.D. Pa. 1985). Served as an expert for defendant-counterclaimant physician as to fraud in the inducement by a computer hardware supplier. Plaintiff had provided capital financing for the purchase. Result: defendant was awarded compensatory damages + $250,000 punitive damages. (D,T)

3. *In re Comprehensive Business Systems,* 119 B.R. 573 (S.D. Ohio 1990). Served as an expert for a secured creditor in a bankruptcy case in which the creditor sought to obtain software still in development for which it had advanced over $2 million in funding. Dr. Shamos opined as to the value of the incomplete software. Result: the creditor was able to purchase the software from the Trustee for $67,500. The Court referred in its opinion to "the testimony of the eminent and impressive Dr. Shamos." (D,R,T)

4. *Levinson Steel Co. v. American Software, Inc. et al.*, Civil Action No. 96-282, W.D. Pa. (1996). Served as an expert for plaintiff in a case involving bad faith estimates of computer processing capacity resulting in delivery of an inadequate system. Result: settlement in favor of plaintiff in an undisclosed amount. Contact: Reed Smith LLP, 225 Fifth Ave., Pittsburgh, PA 15222. (D,R)

5. *ASE Limited v. INCO Alloys International, Inc.*, Civil Action No. 98-1266, (W.D. Pa. 1998). Served as an expert for defendant concerning breach of computer services contract by declaratory judgment plaintiff. Result: determination that defendant was free to seek services from a different vendor. Firm: Reed Smith LLP, 225 Sixth Ave., Pittsburgh, PA 15222. Attorney: Anthony Basinski, Esq. (D,T)

6. *Twentieth Century Fox Film Corp. v. iCraveTV*, 53 U.S.P.Q. 2d 1831 (W.D. Pa. 2000). Served as an expert for Plaintiffs concerning Internet technology used to stream video from U.S. TV stations through web sites in Canada. Result: TRO and preliminary injunction issued against defendants prohibiting continued infringement in the U.S. Firm: Reed Smith LLP. Attorney: Gregory Jordan, Esq. (T)

7. Invited testimony before the British House of Lords, Subcommittee B of the European Union Committee, April 20, 2000. Subject: European regulation of eCommerce. View testimony.

8. *Universal Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), aff'd 273 F.3d 429 (2d Cir. 2001). Served as an expert for plaintiff movie studios concerning accused software for decrypting DVDs in the first case interpreting the Digital Millennium Copyright Act. Result: permanent injunction issued in favor of plaintiffs on August 17, 2000. Contact: William Hart, Esq., Proskauer Rose LLP. View testimony. View opinion. View appellate opinion. (D,T)

9. *MercExchange, L.L.C. v. eBay, Inc. et al.*, Case No. 2:01-CV-736 (E.D. Va. 2001). Served as an expert for defendant eBay in an infringement case concerning U.S. Patent 6,202,051 for Internet auctions. Following Dr. Shamos' reports, Defendants obtained a summary judgment of noninfringement of the subject patent. On the other patents, the case went to the U.S. Supreme Court, which ruled that injunctions are not automatic in patent cases. Contact: Tim Teter, Esq., Cooley LLP. (D,R)

10. *PowerQuest Corp. v. Quarterdeck Corp. et al.*, Case No. 2:97-CV-0783 (D. Utah 1997). Served as an expert for plaintiff PowerQuest in an infringement case concerning U. S. Patents 5,675,769 and 5,796,472 for a method of resizing hard disk partitions. Dr. Shamos testified at the Markman hearing. Case settled when one of the defendants acquired plaintiff. Attorney: Gregg I. Anderson, Esq., formerly at Merchant & Gould, now an Administrative Patent Judge at the Patent Trial and Appeal Board. (R,T)

11. *Sightsound.Com Inc. v. N2K Inc. et al.*, C.A. 98-118 (W.D. Pa. 1998). Served as an expert for defendants, including a subsidiary of Bertelsmann AG, concerning validity of U.S. Patents 5,191,573 and 5,966,440 for distribution of digital audio via telecommunications lines. Case

settled. Firm: Parcher, Hayes & Snyder, (no longer in existence). Contact: Steven M. Hayes, Esq., Simmons Hanley Conroy, LLC, 112 Madison Ave., New York, NY 10016. (D,R)

12. *Freemarkets, Inc. v. B2eMarkets, Inc.*, C.A. 02-162-SLR (D. Del. 2002). Served as an expert witness for plaintiff concerning infringement of U.S. patents 6,216,114 and 6,223,167, concerning methods of conducting electronic auctions. Case settled two weeks after expert attended a demonstration of the accused product. Contact: D. Michael Underhill, Esq., Boies, Schiller & Flexner, LLP, Washington, DC.

13. *Lifecast.com, Inc. v. ClubCorp, Inc.*, AAA Case No. 71Y1170076301 (Dallas, TX). Served as an expert witness for respondent in a case alleging copyright infringement of Internet websites. Testified at arbitration. Result: Complainant's claims denied; award for respondent on counterclaims and for attorney's fees. Contact: Bill Whitehill, Esq., Gardere Wynne Sewell LLP, 1601 Elm St., Dallas, TX 75201. (T)

14. *IP Innovation LLC v. Thomson Learning, Inc. et al.*, Case H-02-2031 (S.D. Tex. 2002). Served as an expert for defendant The Princeton Review, Inc. concerning alleged infringement of U.S. Patent 4,877,404 relating to online delivery of educational courses. Summary judgment of non-infringement obtained for defendant after favorable Markman proceeding. Contact: Peter Vogel, Esq., Gardere Wynne Sewell LLP, 1601 Elm St., Dallas, TX 75201. (R)

15. *Starpay.com LLC et al. v. Visa International Service Association et al.*, Case 3-03-CV-976-L (N.D. Tex. 2003). Served as an expert for defendant Visa concerning alleged infringement of U.S. Patent 5,903,878 relating to online authentication of credit card customers. Dr. Shamos provided the court with a Markman tutorial in 2004 and a non-infringement and invalidity declaration in 2008. Case settled in February 2008. Contact: Stanley Young, Esq., Covington & Burling LLP, 333 Twin Dolphin Drive, Suite 700, Redwood Shores, CA 94065. (D,R,T)

16. *Safeclick LLC v. Visa International Service Association et al.*, Case C-03-5865 (N.D. Cal. 2003). Served as an expert for defendant Visa concerning alleged infringement of U.S. Patent 5,793,028 relating to online authentication of credit card customers. Summary judgment of noninfringement granted for Visa based on expert reports, affirmed after appeal to the Federal Circuit. Contact: Stanley Young, Esq., Covington & Burling LLP, 333 Twin Dolphin Drive, Suite 700, Redwood Shores, CA 94065. (D,R)

17. *Wells Fargo Bank Minnesota, NA et al. v. UBS Warburg Real Estate Securities, Inc.*, Case 02-2849 (192d Judicial District, Dallas Cty., Tex, 2002) and *LaSalle Bank, NA et al. v. UBS Warburg Real Estate Securities, Inc.*, Case 02-2899-G (134th Judicial District, Dallas Cty., Tex, 2002). Served as an expert for defendant UBS Warburg in an electronic discovery matter involving a case of first impression regarding Texas Discovery Rule 196.4 allocating costs of discovery of electronic records. Firm: Gardere Wynne Sewell LLP, 1601 Elm St., Dallas, TX 75201. Contact: Dawn Estes, Esq., Taber, Estes Okon Thorne & Carr PLLC, 3811 Turtle Creek Blvd., Suite 2000, Dallas, TX 75219. (D, R)

18. *American Association of People with Disabilities et al. v. Shelley et al.*, Case No. CV04-1526 FMC (PJWx) (C. D. Calif., 2004). Served as an expert for plaintiff AAPD, which has brought a claim against the California Secretary of State that requiring DRE voting machines to be equipped with audit trails violates the rights of disabled persons. Plaintiffs' application for TRO and preliminary injunction denied. Firm: Howrey LLP, (no longer in existence). Attorney John E. McDermott is now a Magistrate Judge in the Central District of California. (R)

19. *Paul Ware v. Target Corp.*, CA 4:03-CV-0243-HLM (N.D. Ga., 2003). Served as an expert for defendant Target Corp., a large retailer, in a case involving U.S. patent 4,707,592, claiming a method of conducting credit card sales. Case settled during Markman preparations. Contact: Thomas P. Burke, Esq., Ropes & Gray LLP, 1211 Ave. of the Americas, New York, NY 10036.

20. *Viad Corp., v. C. Alan Cordial et al.,* No. 03-1408 (W.D. Pa., filed 2003). Served as an expert for defendants in an action alleging misappropriation of trade secrets relating to software for automating certain aspects of the exhibit booth and trade show industries. Status: case settled immediately before trial, after plaintiff's unsuccessful Daubert challenge of Dr. Shamos. Contact: Barbara Scheib, Esq., Cohen & Grigsby, P.C., 11 Stanwix Street, Pittsburgh, PA 15222. (D,R,T)

21. *Schade et al. v. Maryland State Bd. of Elections et al.*, Case No. C0497297 (Cir. Ct. Anne Arundel Cty. Md., 2004). Served as an expert for defendants in a case challenging the decision of the Board of Elections not to decertify Diebold AccuVote system. Result: Plaintiff's motion for preliminary injunction denied, upheld on appeal. Judge Manck's opinion cites Dr. Shamos' testimony as follows: "the court finds Dr. Shamos, Defendants' expert, to be the true voice of reason and the most credible expert in this matter." The denial of preliminary injunction was upheld by the Maryland Court of Appeals, which commented extensively on Dr. Shamos' testimony in its opinion. Contact: Michael Berman, Esq., (formerly Maryland Deputy Attorney General), Rifkin, Weiner, Livingston, Levitan & Silver, LLC. (R,T)

22. *Wexler et al. v. Lepore et al.*, Case No. 04-80216 (CIV-COHN) (S.D. Fla. 2004) . Served as an expert for defendants, various Florida election supervisors against claim by U.S. Congressman Robert Wexler that use of DRE voting machines without paper audit trails violates the equal protection clause of the U.S. Constitution. Dr. Shamos testified on Oct. 19, 2004. The trial judge rendered judgment in favor of defendants on Oct. 25. Contact: Jason Vail, Esq., then Assistant Attorney General, Department of Legal Affairs, The Capitol, Tallahassee, FL, now at Allen Norton & Blue, PA. Opinion. (T)

23. *Siemens Information and Communication Networks, Inc. v. Inter-Commercial Business Systems, Inc.*, Civil Action 3-03CV2171-L (N.D. Tex. 2004). Served as an expert for defendant against claim of copyright infringement based on reverse-engineered firmware resident in telephone switching systems. Status: case settled shortly after the submission of Dr. Shamos's rebuttal report on non-infringement. Contact: Bill Whitehill, Esq., Gardere Wynne Sewell LLP, 1601 Elm St., Dallas, TX 75201. (R)

24. *Soverain Software LLC v. Amazon.com, Inc.*, C.A. No. 6:04-CV-14 (E.D. Tex. 2004). Served as an expert for plaintiff regarding asserted patents 5,708,780, 5,715,314 and 5,909,492,

relating to the shopping cart paradigm of electronic commerce. Status: settled in Sept. 2005 with Amazon paying $40 million to Soverain and taking a license under the patents in suit. Contact: Ognian Shentov, Esq., Jones Day, 222 E. 41st St., New York, NY 10017. (D,R)

25. *CollegeNET, Inc. v. The Princeton Review, Inc.*, Case '051205KI (D. Ore. 2005). Served as an expert for defendant The Princeton Review, Inc. concerning alleged infringement of U.S. Patent 6,460,042 relating to online delivery of educational courses. Case settled in December 2007. Contact: Peter Vogel, Esq., Gardere Wynne Sewell LLP, 1601 Elm St., Dallas, TX 75201. (R)

26. *CombineNet, Inc. v. VerticalNet. Inc.*, GD 05-018911 (Ct. Common Pleas, Allegheny Cty., PA). Served as an expert for plaintiff in an action for trade secret misappropriation relating to a system for conducting electronic auctions. Plaintiff won in arbitration. Contact: Mark Knedeisen, Esq., K&L Gates LLP, 210 Sixth Avenue, Pittsburgh, PA 15222-2613. (T)

27. *RealSource, Inc. v. Best Buy Co., Inc. et al.*, No. A04-CA-771-LY (W.D. Tex.). Served as an expert for defendant Lowe's Companies, Inc., against a claim of infringement of U.S. patent 5,732,136 relating to validation of point-of-sale debit card transactions. Provided a tutorial to the Court during Markman proceedings concerning debit card technology. Defendants won summary judgment of non-infringement, affirmed by the Federal Circuit. Defendants Lowe's settled and was not involved in the appeal. Contact: Michael S. Connor, Esq., Alston & Bird LLP, Bank of America Plaza, 101 South Tryon St, Suite 4000, Charlotte, NC 28280-4000. (R,T)

28. *DE Technologies, Inc. v. Dell, Inc. et al.*, No. 7:04-CV-00628 (W.D. Va.). Served as an expert for plaintiff DE Technologies, Inc., asserting a claim of infringement of U.S. patents 6,460,020 and 6,845,364, relating to a system for implementing international sales transactions. Case settled after and adverse summary judgment. However, the Court used Dr. Shamos' testimony in its opinion. Contact: David Marder, Esq., Robins Kaplan Miller & Ciresi LLP, 800 Boylston Street, 25th Floor, Boston, MA 02199. (D,R,T)

29. *Eaton Power Quality Corp. v. J.T. Packard & Associates*, No. 05 C 3545 (N.D. Ill. 2005). Served as expert for plaintiff in a claim of software copyright infringement involving a system for configuring industrial uninterruptible power supplies. Case settled in early 2007. Firm: Dewey & LeBoeuf. Contact: Keith P. Schoeneberger, Esq., Pasulka & Associates PC. (D,R)

30. *Taylor et al. v. Onorato et al.*, CA 06-481 (W.D. Pa 2006). Served as an expert for Commonwealth of Pennsylvania defendants in an action seeking to enjoin the use of electronic voting machines in Allegheny County, PA. Dr. Shamos testified at length in a preliminary injunction hearing held April 25-27, 2006 before Judge Lancaster. The injunction was denied on April 28. Suit was subsequently dropped by plaintiffs. Contact: Mark Aronchick, Esq., Hangley Aronchick Segal Pudlin & Schiller, One Logan Square, 18th & Cherry Streets, 27th Floor, Philadelphia, PA 19103. (T)

31. *FedEx Ground Package System, Inc. v. Applications International Corp.*, CA No. 03-1512 (W.D. Pa.). Served as an expert for defendant counterclaiming for copyright infringement and

trade secret misappropriation relating to software for maintaining occupational health and safety records. Dr. Shamos's testimony was excluded because he was unable to perform a side-by-side comparison of the original and accused works. Case has settled. Contact: Ronald Hicks, Esq., Meyer, Unkovic & Scott LLP, 1300 Oliver Bldg., Pittsburgh, PA 15222. (D,R)

32. *NetMoneyIN, Inc. v. Verisign, Inc. et al.*, Cv-01-441-TUC-RCC (D. Ariz.). Served as an expert for defendants Bank of America Merchant Services, Inc. and Wells Fargo Bank, N.A., who are accused of infringing claim 23 of U.S. patent 5,822,737, relating to an electronic payment system. Wells Fargo and Bank of America have settled. Contact: K&L Gates LLP, State Street Financial Center, One Lincoln Street, Boston, Massachusetts 02111-2950. (D,R)

33. *Contois Music Technology, LLC v. Apple Computer, Inc.*, 2:05-CV-163 (D. Vermont, filed Feb. 13, 2006). Served as an expert for plaintiff in an action alleging that the Apple iTunes software infringed U.S. patent 5,864,868, relating to a method for selecting music from an electronic catalog. Case settled after a favorable Markman order. Contact: John Rabena, Esq., Sughrue Mion PLLC, 2100 Pennsylvania Avenue, NW, Suite 800, Washington, DC 20037-3213.

34. *Banfield et al. v. Cortés*, 442 MD 2006 (PA Cmwlth. Ct.). Served as an expert for defendant Secretary of the Commonwealth of Pennsylvania in an action to compel the decertification of all electronic voting machines in Pennsylvania. In February 2008 Defendant successfully repelled an emergency motion for preliminary injunction. In August 2012, the Court denied Petitioners' motion for summary judgment, citing Dr. Shamos's expert report extensively. In October 2013, the Commonwealth Court granted summary judgment for the Secretary. The Pennsylvania Supreme Court affirmed on February 18, 2015. Contact: Steven E. Bizar, Esq., Buchanan Ingersoll & Rooney PC, Two Liberty Place, 50 S. 16th St., Philadelphia, PA 19102-2555. (D,R)

35. *Remote Inventory Systems, Inc. v. WESCO Distribution, Inc.*, AAA Case No. 55 171 00493 05 (Pittsburgh, PA). Served as an expert for respondent in a case alleging misappropriation of trade secrets in a computerized inventory system. Contact: Kirsten Rydstrom, Esq., Reed Smith LLP, 225 Fifth Ave., Pittsburgh, PA 15222. (D,R)

36. *SyncSort, Inc. v. Innovative Routines International, Inc.,* Civil Action No. 04-3623 (WHW) (D. New Jersey). Served as an expert witness for defendant in an action alleging misappropriation of trade secrets embodied in plaintiff's Unix sorting software. Dr. Shamos testified at a bench trial in January 2011. Case settled after an appeal to the Third Circuit was filed. Contact: David R. Fine, Esq., K&L Gates LLP, 17 N. Second Street, 18th Floor, Harrisburg, PA 17101-1507. (D,R,T)

37. *Digital Impact, Inc. v. Bigfoot Interactive, Inc.*, Civil Action C05 00636 (CW) (N.D. Cal.). Served as an expert witness for defendant in an action alleging infringement of U.S. Patent 6,449,634, relating to determining which file formats can be processed by an email client. Result: defendant obtained summary judgment of non-infringement, upheld by the Federal Circuit. Contact: Arthur Dresner, Esq., Duane Morris LLP, 1540 Broadway, New York, NY 10036. (D,R)

38. *Prism Technologies LLC v. Verisign, Inc. et al.*, CA 05-214-JJF (D. Del.). Served as an expert for plaintiff in an action alleging infringement of U.S. Patent 6,516,416, relating to use of a hardware key for authentication over networks. Defendants prevailed on summary judgment of non-infringement, which was upheld on appeal. Firm: Robins Kaplan Miller & Ciresi LLP. Contact: Dirk D. Thomas, Esq., McKool Smith, 1999 K Street, N.W., Suite 600, Washington, DC 20006. (R)

39. *AdvanceMe, Inc. v. RapidPay LLC et al.*, Civil Action 6:05-cv-424 LED (E.D. Tex., Tyler Division). Served as an expert witness for plaintiff in an action alleging infringement of U.S. Patent 6,941,281, relating to an automated payment system for dividing credit card proceeds between a merchant and another party. Testified at a bench trial in July 2007 before Judge Davis, who held the patent infringed but invalid for obviousness. Firm: Paul, Hastings LLP, Five Palo Alto Sq., Palo Alto, CA 94306. Contact: Ronald S. Lemieux, Esq., Singularity LLP, 275 Shoreline Drive, Redwood Shores, CA 94065. (D,R,T)

40. *IBM Corp. v. Amazon.com, Inc.*, CA 9:06-CV-242-RHC (E.D. Tex., Lufkin Div.) and *IBM Corp. v. Amazon.com, Inc.*, CA 6:06-CV-452-LED (E.D. Tex., Marshall Div.). Served as an expert for IBM in related actions alleging infringement of U.S. Patents 5,319,542, 5,442,771, 5,446,891, 5,796,967 and 7,072,849, all concerning methods of conducting electronic transactions, and a counterclaim for infringement of U.S. Patent 5,826,258, concerning a method for querying semistructured data. Case settled early in discovery when the parties cross-licensed each other's patents. Contact: Mark J. Ziegelbein, Esq., Dentons US LLP, 2000 McKinney Ave., Suite 1900, Dallas, TX 75201-1858.

41. *The MathWorks, Inc. v. COMSOL AB et al.*, CA 6:06-CV-334 (E.D. Tex., Tyler Division). Served as an expert for plaintiff The MathWorks, providers of the mathematical software system MATLAB, in an action alleging copyright infringement and infringement of U.S. Patents 7,051,338 and 7,181,745 concerning methods for invoking object methods from external environments. After trial, the case settled with defendant admitting infringement, paying $12,000,000 in damages and waiving appeal rights. Contact: Krista Schwartz, Esq., Jones Day, 77 W. Wacker Dr., Chicago, IL 60601-1692.

42. *Avante Int'l. Technology Corp. v. Diebold Election Systems et al.,* Case 4:06-CV-0978 TCM (E.D. Mo., Eastern Division). Served as an expert for defendants Sequoia Voting Systems and Premier Election Systems in an action alleging infringement of U.S. Patents 6,892,944, 7,036,730 and 7,077,313 concerning electronic voting technology. Dr. Shamos testified at a 5-day trial in February 2009. Result: The jury found Plaintiff's asserted claims invalid as anticipated and obvious. Contact: Peter T. Ewald, Esq., Oliff & Berridge, PLC, 277 South Washington Street, Suite 500, Alexandria, VA 22314. (D,R,T)

43. *Netcraft Corp. v. eBay, Inc. and PayPal, Inc.*, Case 3:07-cv:00254-bbc (W.D. Wisc. 2007). Served as an expert for defendants in an action alleging infringement of U.S. Patents 6,351,739 and 6,976,008 concerning methods of billing for ecommerce transactions over the Internet. Defendants were granted summary judgment of non-infringement on Dec, 10, 2007, upheld on appeal. Firm: Irell & Manella LLP, 180 Avenue of the Stars, Los Angeles, CA

90067. Contact: Kenneth Weatherwax, Esq., Goldberg, Lowenstein & Weatherwax LLP, 1925 Century Park East, Suite 2120, Los Angeles, CA 90067.

44. *ACLU of Ohio et al. v. Brunner et al.*, Case 1:09 CV 0145 (N.D. Ohio 2008). Served as an expert witness in an action alleging that the use of central count optical scan voting should not be permitted in Cuyahoga County, as had been ordered by the county board of elections. A preliminary injunction was denied in February 2008. The case became moot and was dismissed in May 2008 when the Ohio Legislature granted by statute the relief requested by plaintiff, prohibiting the use of central count opscan in Cuyahoga County. Contact: Meredith Bell-Platts, Esq., ACLU Voting Rights Project, 2600 Marquis One Tower, Atlanta, GA 30303. (R)

45. *Ariba, Inc. v. Emptoris, Inc.*, Civil Action 9:07-CV-90-RHC (E.D. Tex. 2007). Served as an expert for Ariba in an action alleging infringement of U.S. Patents 6,216,114 and 6,499,018, relating to the conduct of electronic auctions. Dr. Shamos testified in a jury trial on infringement and validity. Result: verdict finding all asserted claims valid and willfully infringed. Contact: Robert Fram, Esq., Covington & Burling LLP, One Front St., San Francisco, CA 94111. (D,R,T)

46. *EpicRealm Licensing, LP v. Autoflex Leasing Inc. et al.*, CA 5:07-CV-125 (E.D. Tex. 2005). Served as an expert for defendant Herbalife International of America, Inc. in an action alleging infringement of U.S. patents 5,894,554 and 6,415,335, relating to a system for managing generation of dynamic Internet web pages. All original defendants settled. See also the Oracle case below. Contact: Ognian Shentov, Esq., Jones Day, 222 E. 41st St., New York, NY 10017. Also served as an expert for defendant FriendFinder in a separate trial in this action. After a jury trial before Judge Folsom, the patents were found valid and infringed, but the jury awarded only $1.1M, the smallest amount testified to by defendant's damages expert. Contact: Michael J. Sacksteder, Esq., Fenwick & West LLP, 555 California St., San Francisco, CA 94104. (D,R,T)

47. *Oracle Corporation v. EpicRealm Licensing, LP,* CA 2-06-414 (D. Del. 2006), later *Oracle Corporation v. Parallel Networks, LLC.* Served as an expert for Oracle in a declaratory judgment alleging invalidity of U.S. patents 5,894,554 and 6,415,335, relating to a system for managing generation of dynamic Internet web pages. The patents are the same as those in the EpicRealm case, above. Oracle obtained summary judgment of non-infringement, reversed on appeal to the Federal Circuit. Case settled in May 2011 on the eve of trial. Firm: Kilpatrick Townsend & Stockton, LLP, 379 Lytton Ave., Palo Alto. CA 94301. Contact: Theodore T. Herhold, Singularity LLP, 275 Shoreline Drive, Redwood Shores, CA 94065. (D,R)

48. *Saulic v. Symantec Corporation et al.*, Case No. SA CV 07-610 AHS (C.D. Cal., Santa Ana Division, 2007). Served as an expert for defendant Symantec in a removal action alleging violation of California Civil Code §1747.8, relating to the collection of personal identification information in connection with credit card transactions. Case settled. Original firm: Heller Ehrman. Contact: Chad R. Fuller, Esq., Troutman Sanders LLP, 11682 El Camino Real, Suite 400, San Diego, CA 92121. (R)

49. *Gusciora et al. v. McGreevey et al.* (now *Gusciora v. Christie*), Docket No. MER-L-2691-04 (N.J. Super., Mercer County). Served as an expert for defendants, including the Governor and Attorney General of New Jersey, in a case alleging that the state's AVC Advantage voting machines are unconstitutionally insecure. A bench trial was held from January-May, 2009 before Judge Linda Feinberg. The Court's opinion adopts Dr. Shamos' testimony and comments on it extensively. Affirmed on appeal in October 2013. Contact: Leslie Gore, Esq., Asst. Atty. Gen'l., 25 Market Street, P.O. Box 112, Trenton, NJ 08625. (D,R,T)

50. *R.R. Donnelley & Sons Company v. Quark, Inc. et al.*, C.A. No. 06-00032-JJF (D. Del.). Served as an expert for plaintiff R.R. Donnelley in a case alleging infringement of U.S. Patents 6,205,452, 6,327,599, 6,844,940 and 6,952,801, relating to book assembly, imposition of graphics and control of electronic presses. Case has settled. Contact: Stuart W. Yothers, Esq., Ropes & Gray LLP, 1251 Avenue of the Americas, New York, NY 10020.

51. *MOAEC, Inc. v. Pandora Media, Inc. et al.*, Case No. 07-cv-654-bbc (W.D. Wisc.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 5,969,283, 6,232,539, 6,953,886 and 7,205,471, relating to systems for organizing and retrieving digital music. Two defendants obtained summary judgment of noninfringement; the remaining defendant settled. Contact: Joshua Krumholz, Esq., Holland & Knight, LLP, 10 St. James Avenue, 11th Floor, Boston, MA 02116. (D,R)

52. *Web.com, Inc. v. The Go Daddy Group, Inc.*, Case No. CV07-01552-PHX-MHM (D. Ariz.). Served as an expert for defendant in a case alleging infringement of U.S. Patents 6,654,804, 6,789,103, 6,842,769 and 6,868,444, relating to methods for managing configuration of web servers and provision of Internet services. Case has settled. Firm: Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304. Contact: Richard G. Frenkel, Esq., Latham & Watkins LLP, 140 Scott Drive, Menlo Park, CA 94025.

53. *Hummel et al. v. Dynacraft BSC, Inc. et al.*, Case No. CV 052214 (Cal. Super. Marin Cty.). Served as an expert for defendants in an action alleging breach of contract for web hosting services. Dr. Shamos provided four hours of trial testimony. Result: verdict for the defense. Contact: Joe B. Harrison, Esq., Gardere Wynne Sewell LLP, 1601 Elm St., Suite 3000, Dallas, TX 75201. (T)

54. *Tegg Corp. v. Beckstrom Electric Co. et al.*, Civil Action No. 2:08-CV-00435-NBF (W.D. Pa.). Served as an expert for defendants in a case alleging infringement of copyright in computer software for administering field maintenance of electrical equipment. Case has settled. Original firm: Reed Smith LLP. Contact: Richard D. Kelley, Esq., Bean Kinney & Korman, 2300 Wilson Blvd., Suite 700, Arlington, VA 22220.

55. *Cordance Corporation v. Amazon.com, Inc.*, Civil Action No. 06-491-MPT (D. Del.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 5,862,525, 6,088,717 and 6,757,710, relating to an infrastructure for conducting online transactions. In August 2009 a jury found the '717 patent valid but not infringed and the '710 patent infringed but invalid. The finding of invalidity of the '710 patent was vacated by the Court on judgment as a matter of law. The Federal Circuit reversed and reinstated the jury's finding. Contact: Robert

M. Abrahamsen, Esq., Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210. (D,R, T)

56. *Anthurium Solutions, Inc. v. MedQuist, Inc. et al.*, Case No. 2:07-vcv-484 (DF/CE) (E.D. Tex.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patent 7,031,998, relating to a distributed workflow system. Case settled ten days after responsive expert reports were served. Contact: Joshua Krumholz, Esq., Holland & Knight, LLP, 10 St. James Avenue, 11th Floor, Boston, MA 02116. (R)

57. *Performance Pricing, Inc. v. Google, Inc. et al.*, Case No. 2:07-cv-432(LED) (E.D. Tex.). Served as an expert for defendant Yahoo! in a case alleging infringement of U.S. Patent 6,978,253, relating to determining prices for items sold online. Case has settled as to defendant Yahoo!. Contact: Michael A. Jacobs, Esq., Morrison & Foerster LLP, 425 Market Street, San Francisco, CA 94105. Also served as an expert for remaining defendants Google and AOL. In March 2010 the Court granted defendants' motion for summary judgment of noninfringement, affirmed by the Federal Circuit. Contact: David A. Perlson, Esq., Quinn Emanuel Urquhart & Sullivan, LLP, 50 California Street, San Francisco, CA 94111. (D,R)

58. *Nationwide Power Solutions, Inc. et al., v. Eaton Electrical Inc.*, Case No. CV-8:07-0883-JVS (C.D. Cal.). Served as an expert for defendant/counterclaimant Eaton in a case alleging antitrust violations by Eaton arising out of proprietary servicing software in its uninterruptible power supplies. Case has settled. Contact: James L. Day, Esq., Latham & Watkins LLP, 505 Montgomery Street, Suite 2000 San Francisco, CA 94111.

59. *CBS Interactive, Inc. v. Etilize, Inc.*, Case No. C -6-05378 (MHP) (N.D. Cal.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 6,714,933 and 7,082,426, relating to web crawling technology to aggregate product information. Defendant consented to an injunction against further infringement and the case settled. Firm: Winston & Strawn, LLP, 101 California Street, San Francisco, CA 94111. Contact: Glenn E. Westreich, Esq., Hayes and Boone, LLP, 2033 Gateway Place, San Jose, CA 95110.

60. *Geographic Services, Inc. v. Anthony Collelo*, Case 2008-9961 (Fairfax Cty., Va.). Served as an expert for plaintiff in a case alleging misappropriation of trade secrets involving determining and proofing geographic names as applied to maps and satellite imagery. Case was dismissed by Judge Ney on technical legal grounds at the close of Plaintiff's case. The Virginia Supreme Court reversed and remanded the case for further proceedings. Case has settled. Contact: Mark W. Wasserman, Esq., Reed Smith LLP, 3110 Fairview Park Drive, Suite 1400, Falls Church, VA 22042. (D,R,T)

61. *ODS Technologies, LP v. Magna Entertainment Corp., et al.*, CV 07-03265 DDP (D. Del.). Served as an expert for defendants in a case alleging infringement of U.S. Patents 5,830,068, 6,004,211, 6,089,981, 6,554,709 and 7,229,354, relating to off-track wagering systems and methods for restricting wagering based on location. Dr. Shamos submitted a declaration in support of summary judgment. Case settled before expert reports were

due. Contact: Virginia DeMarchi, Esq., Fenwick & West, LLP, 801 California Street, Mountain View, CA 94041. (R)

62. *Gannett Satellite Information Network, Inc. v. Office Media Network, Inc.*, C.A. No. 08-96-GMS (D.Del.). Served as an expert for defendant in a case alleging infringement of U.S. Patents 6,288,688, 6,622,826, 6,981,576 and 7,270,219, relating to display of advertising information on screens in elevators. Case settled shortly after Dr. Shamos's deposition. Contact: Steven R. Trybus, Esq., Jenner & Block LLP, 353 N. Clark St., Chicago, IL 60654. (D,R)

63. *Avante Int'l. Technology Corp. v. Premier Election Solutions et al.,* Case 4:06-CV-091367-ERW (E.D. Mo., Eastern Division). Served as an expert for defendants Sequoia Voting Systems and Premier Election Systems in an action alleging infringement of U.S. Patents 7,422,150, and 7,431,209 concerning electronic voting technology. Case settled in December 2009. Contact: Peter T. Ewald, Esq., Oliff & Berridge, PLC, 277 South Washington Street, Suite 500, Alexandria, VA 22314. (R)

64. *Accenture Global Services GmbH et al. v. Guidewire Software, Inc.*, Civ. No. 07-826-SLR (D. Del.). Served as an expert for Accenture in a case alleging misappropriation of trade secrets and infringement of U.S. Patents 7,013,284 and 7,017,111, relating to automated insurance claim handling. The District Court found the asserted system claims invalid under 35 U.S.C. § 101, affirmed by the Federal Circuit at 2011-1486. Case settled in Oct. 2011. Original firm: Morrison & Foerster, LLP. Contact: L. Scott Oliver, Esq., K&L Gates LLP, 630 Hansen Way, Palo Alto, CA 94304. (D,R)

65. *Alexsam, Inc. v. Evolution Benefits, Inc. et al.,* Case No. 2:07cv288-TJW (E.D. Tex.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patent 6,000,608, relating to multifunction epayment cards. Case settled four weeks after Dr. Shamos's deposition. Original firm: Wolf, Greenfield & Sacks, P.C. Contact: James Foster, Esq., Hayes Messina Gilman Hayes LLC, 200 State St., 6th Floor, Boson, MA 02109. (D,R)

66. *Motivation Innovations, LLC v. DSW Inc. et al.*, C.A. No. 08-334-SLR (D. Del.). Served as an expert for defendant DSW, Inc. in a case alleging infringement of U.S. Patent 5,612,527, relating to a system for redeeming discount offers at point of sale. Case has settled. Contact: Drew Blatt, Ph.D., Esq., Wood, Heron & Evans LLP, 2700 Carew Tower 441 Vine Street Cincinnati, Ohio 45202.

67. *Discovery Communications, Inc. v. Amazon.com, Inc.*, C.A. No. 09-178-ER (D. Del.). Served as an expert for plaintiff Discovery Communications in a case alleging infringement of plaintiff's U.S. Patents 5,986,690, 6,657,173, 7,298,851, 7,299,501, 7,336,788 and 7,401,286, relating to electronic book viewers and electronic book selection and delivery systems, and defendant-counterclaimant's U.S. Patents 6,029,141 and 7,337,133, relating to Internet-based customer referral systems. Case has settled. Contact: Brent P. Lorimer, Esq., Workman | Nydegger, 1000 Eagle Gate Tower, 60 East South Temple Salt Lake City, UT 84111.

68. *Amazon.com v. Discovery Communications, Inc.*, No. 2:09-cv-0681-RSL (W.D. Wash.). Served as an expert for defendant Discovery Communications in a case alleging

infringement of U.S. Patents 6,006,225 and 6,169,986, relating to refinement of online search queries, and U.S. Patents 6,266,649 and 6,317,722., relating to generation of online recommendations. Case has settled. Contact: Brent P. Lorimer, Esq., Workman | Nydegger, 1000 Eagle Gate Tower, 60 East South Temple Salt Lake City, UT 84111.

69. *IMX, Inc. v. E-Loan, Inc. and Banco Popular North America, Inc.*, No. 09-cv-20965 (S.D. Fla.). Served as an expert for defendants in a case alleging infringement of U.S. Patent 5,995,947, relating to an interactive loan processing and mortgage trading system. Case was stayed pending reexamination. On appeal after reexamination, all but four of the asserted claims were cancelled. In CBM2015-00012, all asserted claims were found unpatentable under §101. Case has settled. Contact: Samuel A. Lewis, Esq., Feldman Gale, PA, One Biscayne Tower, 30th Floor, 2 South Biscayne Blvd., Miami, FL 33131. (D,R)

70. *Soverain Software LLC v. CDW Corp. et al.*, C.A. No. 6:07-CV-511 (E.D. Tex.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 5,715,314, 5,909,492, and 7,272,639, relating to methods of conducting electronic commerce. All defendants settled except Newegg, Inc. Dr. Shamos testified on validity at a jury trial in April 2010. Result: all claims valid; the '314 and '492 claims infringed, with a running royalty assessed against Newegg. After trial, the Court found the '639 patent infringed as a matter of law. In January 2013 the Federal Circuit found the asserted claims obvious as a matter of law, The Supreme Court declined review. Contact: Ognian Shentov, Esq., Jones Day, 222 E. 41st St., New York, NY 10017. (D,R,T)

71. *Netcraft Corp. v. AT&T Mobility LLC et al.*, C.A. No. 07-651-GMS (D. Del.). Served as an expert for defendants in a case alleging infringement of U.S. Patents 5,974,221, 6,351,738 and 6,411,940, relating to electronic commerce billing methods. Case settled two months after Dr. Shamos's deposition. Contact: H. Jonathan Redway, Esq., Dickinson Wright PLLC, 1875 Eye St., Washington, DC 20006. (D,R)

72. *ValueClick, Inc. v. Tacoda, Inc., AOL, LLC and Platform-A, Inc.*, Case No. 2:08-cv-04619 DSF (JCx) (C.D. Cal.). Served as an expert for defendants in a case alleging infringement of U.S. Patents 5,848,396 and 5,991,735, relating to software and methods for creating psychographic profiles of network users. Case settled in May 2010. Original firm: Orrick, Herrington & Sutliffe, LLP. Contact: Paul R. Gupta, Esq., DLA Piper, 1251 Avenue of the Americas, New York, NY 10020.

73. *SP Technologies, Inc. v. Garmin Limited et al.*, Civil Action No. 08-CV-3248 (N.D. Ill.). Served as an expert for defendant TomTom, Inc. in a case alleging infringement of U.S. Patent 6,784,873, relating to graphical keyboards on touchscreens. Defendants prevailed on summary judgment of invalidity. Contact: Brian Pandya, Esq., Wiley Rein LLP, 1776 K Street NW, Washington DC 20006. (D,R)

74. *ePlus, Inc. v. Lawson Software, Inc.*, Civil Action No. 3:09-cv-620 (E.D. Va.). Served as an expert for defendant in a case alleging infringement of U.S. Patents 6,023,683, 6,055,516 and 6,505,172, relating to electronic procurement systems. Dr. Shamos testified at a jury trial in Richmond in January 2011. Result: No infringement as to most accused configurations;

infringement as to others. Past damages were precluded by the Court. On appeal. the Federal Circuit found the system claims invalid as indefinite. Contact: Daniel McDonald, Esq., Merchant & Gould PC, 3200 IDS Center, 80 South Eighth Street, Minneapolis, MN, 55402. (D,R,T)

75. *Bed Bath & Beyond, Inc. v. Sears Brands*, LLC, Civil Action 08 CV 5839-SDW-MCA (D. N.J.). Served as an expert for plaintiff in a declaratory judgment action regarding alleged infringement of U.S. Patent 5,970,474, relating to retail gift registry systems. Case has settled. Contact: William Mentlik, Esq., Lerner David Littenberg, Krumholz & Mentlik LLP, 600 South Avenue West, Westfield, NJ 07090. (D,R)

76. *Transauction, LLC v. eBay, Inc.*, Case No. 3:09-cv-3705-SJ (N.D. Cal.). Served as an expert for defendant in a case alleging infringement of U.S. Patent 7,343,339, relating to guarantees in online auctions. Case settled after expert reports were submitted. Firm: Irell & Manella LLP, 1800 Avenue of the Stars, Suite 900, Los Angeles, CA 90067. Contact: Peter E. Gratzinger, Esq., Munger, Tolles & Olson LLP, 355 South Grand Avenue, Los Angeles, CA 90071. (R)

77. *SDG Corporation v. Patrizzi & Co. Auctioneers SA et al.*, ICDR Case No. 50 117 T 00313 09 (Int'l. Centre for Dispute Resolution). Served as an expert for claimant in an arbitration alleging breach of contract to produce software for operating online auctions. Dr. Shamos testified at arbitration in October 2010. Award for SDG on all claims and denial of all of Patrizzi's counterclaims. Contact: Bruce Fox, Esq., Obermayer Rebmann Maxwell & Hippel LLP, One Mellon Center, Suite 5240, Pittsburgh, PA 15219. (D,R,T)

78. *Walker Digital, LLC v. Capital One Services, LLC et al.*, Civil Action 1:10cv212 (JFA) (E.D. Va.). Served as an expert for defendants in a case alleging infringement of U.S. Patents 5,970,478 and 6,374,230, relating to customizing and pricing credit card accounts. Defendants prevailed on summary judgment of non-infringement supported by a declaration from Dr. Shamos. Affirmed by the Federal Circuit on July 28, 2011. Contact: Charles S. Barquist, Esq., Morrison & Foerster LLP, 555 West Fifth Street, Suite 3500, Los Angeles, CA 90013. (R)

79. *Voter Verified, Inc. v. Premier Election Solutions, Inc. et al.*, Case No. 6:09-cv-1968-19KRS (M.D. Fla.). Served as an expert for defendants, manufacturers of voting equipment, in a case alleging infringement of U.S. Patents 6,769,613 and RE40,449, relating to paper trail verification of ballots. The Court denied a Daubert motion to exclude testimony by Dr. Shamos. Summary judgment of non-infringement granted July 28, 2011, affirmed by the Federal Circuit on November 5, 2012. All claims of the '449 patent were found non-statutory by the Federal Circuit in 2018. Contact: Robert M. Evans, Jr., Esq., Stinson LLP, 7700 Forsyth Blvd. Suite 1100, St. Louis, MO 63105. (R)

80. *Elder et al. v. National Conference of Bar Examiners*, No. C 11-00199 SI (N.D. Cal.). Served as an expert for disabled plaintiffs in a case seeking an injunction to permit them to take the bar examination in electronic format. Preliminary injunction granted Feb. 16, 2011. Plaintiff took the bar exam, passed and was awarded $224,000 in attorney's fees. Contact: Daniel F.

Goldstein, Esq., Brown, Goldstein & Levy, LLP, 120 E. Baltimore St., Suite 1700, Baltimore, MD 21202. (R)

81. *Ameranth, Inc. v. Menusoft Systems Corp., et al.*, Civil Action 2-07-CV-271 TJW/CE (E.D. Tex.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 6,384,850, 6,871,325 and 6,982,733, relating to synchronous updating of restaurant menus on wireless devices. After trial, the jury found the patents not infringed. Case settled while an appeal to the Federal Circuit was pending. Contact: John W. Osborne, Esq., Osborne Law LLC, 33 Habitat Lane, Cortlandt Manor, NY 10567. (D,R,T)

82. *BuyFigure.com, Inc. v. Autotrader.com et al.*, Case No. 06391 (Ct. of Common Pleas of Philadelphia County, PA, 2010). Served as an expert for defendants in a case alleging misappropriation of trade secrets concerning a method of selling automobiles over the Internet. Summary judgment was granted in Defendants' favor in August 2012. Contact: Howard D. Scher, Esq., Buchanan Ingersoll & Rooney, P.C., Two Liberty Place, 50 S. 16th Street, Philadelphia, PA 19102. (R)

83. *Soverain Software LLC v. J.C. Penney Corp., Inc. et al.*, C.A. No. 6:09-CV-274 (E.D. Tex.). Served as an expert for plaintiff on validity issues in a case alleging infringement of U.S. Patents 5,715,314, 5,909,492, and 7,272,639, relating to methods of conducting electronic commerce. The '639 patent was dropped before trial and all defendants settled except Avon Products and Victoria's Secret. After trial, the jury found all claims valid and infringed, and awarded damages of $9.2 million against Victoria's Secret and $8.7 million against Avon. Contact: Robert B. Wilson, Esq., Quinn Emanuel Urquhart & Sullivan, LLP, 51 Madison Avenue, 22nd Floor, New York, NY 10010. (D,R,T)

84. *AOL, LLC, et al. v. Yahoo! Inc. et al.*, No. 09 Civ. 3774 (WHP) (S.D.N.Y). Served as an expert for declaratory judgment plaintiff AOL in a case alleging infringement of U.S. Patents 6,078,866, 6,269,361, 6,546,386, 6,907,566, 7,043,483, 7,107,264, 7,373,599, and 7,702,541, relating to online advertising placement and targeted e-commerce. Case settled in Feb. 2011. Original firm: Orrick, Herrington & Sutliffe LLP. Contact: William B. Tabler II, Esq., Flextronics, 6201 America Center Drive, San Jose, CA 95002.

85. *Accenture Global Services GmbH et al. v. Guidewire Software, Inc.*, Civ. No. 09-848-SLR (D. Del.). Served as an expert for Accenture in a case alleging infringement of U.S. Patent 7,617,240, relating to automated insurance claim handling. Case settled in Oct. 2011. Original firm: Morrison & Foerster, LLP. Contact: L. Scott Oliver, Esq., K&L Gates LLP, 630 Hansen Way, Palo Alto, CA 94304. (D,R)

86. *Amdocs (Israel) Limited v. Openet Telecom, Inc. et al.*, Case 1:10-cv-00910-LMB-TRJ (D. Del.). Served as an expert for Defendant Openet in a case alleging infringement of U.S. Patents 6,836,797 and 7,631,065, relating to aggregated billing for network services. Summary judgment of non-infringement granted in favor of Defendants in Sept. 2012. The Court's opinion cites Dr. Shamos' testimony. Judgment reversed on appeal in 2014, but on remand, all claims were invalidated as claiming non-statutory subject matter. After a second appeal, the

§101 ruling was reversed. Case settled during trial in 2018. Contact: Kevin Anderson, Esq., Duane Morris LLP, 505 9th Street, N.W., Suite 1000, Washington, DC 20004-2166 (D,R)

87. *Cross-Atlantic Capital Partners, Inc. v. Facebook, Inc. et al.*, Case 07-CV-2768 JP (E.D. Pa.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patent 6,519,629, relating to establishment of online communities. Asserted claims were cancelled upon reexamination. Case has been dismissed. Original firm: McShea/Tecce PC. Contact: Frederick Tecce, Esq., Panitch Schwarze Belisario & Nadel LLP, One Commerce Square, 2005 Market Street, Suite 2200, Philadelphia, PA 19103. (R)

88. *Chavez et al. v. Bennett et al.*, CV 2006-007000 (Ariz. Super., Maricopa Cty.). Served as an expert for defendant Secretary of State of Arizona and county defendants in a case alleging that the electronic voting systems used in Arizona violated the rights of voters. Case was voluntarily dismissed by plaintiffs in May 2011. Contact: Laurence G. Tinsley, Jr., Esq, Senior General Counsel, Maricopa County Office of General Litigation Services, 301 W. Jefferson St., Phoenix, AZ 85003.

89. *Bonnette v. District of Columbia Court of Appeals and National Conference of Bar Examiners*, No. 11-cv-01053-CKK (D. D.C.). Served as an expert for a disabled plaintiff in a case seeking a preliminary injunction permitting her to take the bar examination in electronic format. Injunction granted. Case subsequently settled with Plaintiff receiving $141,000 in attorneys' fees and costs. Contact: Daniel F. Goldstein, Esq., Brown, Goldstein & Levy, LLP, 120 E. Baltimore St., Suite 1700, Baltimore, MD 21202.

90. *Jones v. National Conference of Bar Examiners et al.*, No. 5:11-cv-00174-cr (D. Vermont). Served as an expert for a disabled plaintiff in a case seeking an injunction permitting to take the bar examination using assistive technology. The preliminary injunction was granted. Plaintiff was awarded $275,000 in attorneys' fees and costs. Contact: Daniel F. Goldstein, Esq., Brown, Goldstein & Levy, LLP, 120 E. Baltimore St., Suite 1700, Baltimore, MD 21202. (R)

91. *AlmondNet, Inc. v. Microsoft Corporation*, Case 10-CV-298 (W.D. Wisc.). Served as an expert for plaintiff and counterclaim defendant AlmondNet in a case alleging infringement of U.S. Patents 6,973,436, 7,072,853, 7,454,364 and 7,822,637 by Microsoft, relating to bidding for Internet ad placement, and infringement of U.S. Patent 6,632,248 by AlmondNet, relating to customization of network documents via a unique user identifier. Microsoft obtained summary judgment of non-infringement. Contact: Meredith Zinanni, Esq., Kirkland & Ellis LLP, 300 N. LaSalle, Chicago, IL 60604.

92. *Kelora Systems, LLC. v. Target Corporation et al.*, Case 10-CV-683 (W.D. Wisc.). Served as an expert for defendant Mason Companies, Inc. in a case alleging infringement of U.S. Patent 6,275,821, relating to guided parametric searching in online catalogs. Case settled as to this defendant in July 2011. The Court granted summary judgment of invalidity and non-infringement as to the other defendants, affirmed by the Federal Circuit. Contact: Shane A. Brunner, Esq., Merchant & Gould, 10 East Doty St., Suite 600, Madison, WI 53703.

93. *TNS Media Research, LLC et al. v. TRA Global, Inc.*, Case 1:2011-CV-4039 (SAS) (S.D. N.Y.). Served as an expert for declaratory judgment plaintiffs in case alleging infringement of U.S. Patent 7,729,940, relating to anonymous matching of program viewing data from television set-top boxes with purchase data from other sources. Patentee's motion for preliminary injunction was denied on Sept. 23, 2011. Plaintiffs' motion for summary judgment of non-infringement was granted on October 3, 2013. Reversed and remanded by the Federal Circuit. Contact: Michael Albert, Esq., Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210. (R)

94. *Accenture Global Services GmbH et al. v. Guidewire Software, Inc.*, Case 3:11-03563-JSW (N.D. Cal.); *Guidewire Software, Inc. v. Accenture PLC et al.*, Case 4:11-cv-04686-LB (N.D. Cal.). Served as an expert for Accenture in related cases alleging infringement by Guidewire of U.S. Patents 6,574,636, 7,409,355 and 7,979,282, relating to systems for insurance claim handling and alleging infringement by Accenture of U.S. Patents 5,630,069, 5,734,837, 6,058,413 and 6,073,109, relating to workflow management systems. Cases settled in Oct. 2011. Contact: Colleen Garlington, Esq., Kirkland & Ellis LLP, 300 N. LaSalle St., Chicago, IL 60604.

95. *XPRT Ventures, LLC v. eBay, Inc. et al.*, C.A. 1:2010-cv-595 (SLR) (D. Del.). Served as an expert for Defendants eBay and PayPal in a case alleging infringement of U.S. Patents 7,483,856, 7,512,563, 7,567,937, 7,599,881, 7,610,244, 7,627,528, relating to methods of paying for items purchased through electronic auctions. Case has settled. Contact: Adrian Percer, Esq., Weil, Gotshal & Manges, LLP, 201 Redwood Shores Parkway, Redwood Shores, CA 94065. (D,R)

96. *Rich Media Club, LLC et al. v. Nikolai Mentchoukov et al.*, Civil No. 2:11-cv-01202-SA (D. Utah). Served as an expert for Plaintiffs in a case alleging breach of an employment contract, unfair competition concerning systems for placing advertisements on web pages and infringement of U.S. Patent 7,313,590, relating to communication between client and server computers without requiring a browser. Contact: Jared Richards, Esq., Bennett Tueller Johnson & Deere, LLC, 3165 East Millrock Drive, Suite 500, Salt Lake City, Utah 84121. (R)

97. *Franklin Inventions LLC v. Election Systems & Software, Inc.*, Case No: 2:09-cv-377 (E.D. Tex.). Served as an expert for Defendants in a case alleging infringement of U.S. Patents 6,986,999, 7,243,846 and 7,575,164, relating to voter-verifiable voting systems. Case settled after a declaration concerning invalidity was submitted by Dr. Shamos. Contact: Robert M. Evans, Jr., Esq., Lewis Rice LLC, 600 Washington Avenue, Suite 2500, St. Louis, MO 63101. (R)

98. *Illinois Computer Research, LLC v. HarperCollins Publishers, LLC, et al.*, Case No.: 10-cv-9124 (S.D.N.Y). Served as an expert for Defendants in a case alleging infringement of U.S. Patent 7,111,252, relating to limiting access to electronic books. Case settled after Markman. Contact: Brian S. Rosenbloom, Esq., Rothwell, Figg, Ernst & Manbeck, P.C., 607 14th Street, N.W., Suite 800, Washington, DC 20005. (R)

99. *Realtime Data, LLC d/b/a IXO v. Morgan Stanley et al.,* Case No.: 11 Civ. 6696 (RJH), *Realtime Data, LLC d/b/a IXO v. CME Group Inc. et al.,* Case No.: 11 Civ. 6701 (RJH), *Realtime Data, LLC d/b/a IXO v. Thompson Reuters, et al.,* Case No.: 1:2011-cv-06704 (RJH) (S.D.N.Y). Served as an expert for Plaintiff in three consolidated cases alleging infringement of U.S. Patents 7,417,568, 7,714,747, and 7,777,651, relating to compression and decompression of financial data streams. Summary judgment granted for defendants, upheld by the Federal Circuit. Contact: Dirk D. Thomas, Esq., McKool Smith, 1999 K Street, N.W., Suite 600, Washington, DC 20006. (D,R,T)

100. *Mulhern Belting, Inc. v. Tele-Data Solutions, Inc.*, Civil Action L-2258-10 (Sup. Ct. Bergen Cty. NJ). Served as an expert for defendant Vertical Communications, Inc. in a case alleging breach of contract and fraud in connection with the installation of an integrated voice-over-IP (VoIP) telecommunications system. Case has settled. Contact: John J. Abromitis, Esq., Courter, Kobert & Cohen P.C., 1001 Route 517, Hackettstown, NJ 07840. (R)

101. *Decision Support, LLC v. Election Systems & Software, Inc.*, Case No: 3:10cv90 (W.D. N.C.). Served as an expert for Defendants in a case alleging infringement of U.S. Patent 7,497,377, relating to electronic voter registration and pollbook systems. Case has settled. Contact: Robert M. Evans, Jr., Esq., Lewis Rice LLC, 600 Washington Avenue, Suite 2500, St. Louis, MO 63101. (R)

102. *Rovi Corporation et al. v. Amazon.com, Inc. et al.*, Case No. 11-cv-00003-RGA (D. Del.). Served as an expert for Plaintiffs in a case alleging infringement of U.S. Patents 5,988,078, 6,275,268, 6,769,128, 7,493,643 and 7,603,690, relating to customized on-screen television guides. The parties stipulated to entry of judgment of noninfringement. Contact: Ragesh L. Tangri, Esq., Durie Tangri LLP, 217 Leidesdorff Street, San Francisco, CA 94111.

103. *Certain Products Containing Interactive Program Guide and Parental Control Technology*, USITC Inv. No. 337-TA-820. Served as an expert for Complainants Rovi Corporation et al. and against Vizio, Inc. et al. in an International Trade Commission proceeding involving alleged infringement of U.S. Patents 6,701,523, 7,047,547, 7,493,643 and RE41,993, relating to v-chips and electronic TV program guides. Case has settled. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304. (R)

104. *Rovi Corporation et al. v. Roku, Inc.*, Case No. 12-cv-2185 EJD (N.D. Cal.). Served as an expert for Plaintiffs in a case alleging infringement of U.S. Patent 6,898,762, relating to a client/server electronic television program guide. Voluntarily dismissed by plaintiff without prejudice. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304.

105. *Rovi Corporation et al. v. LG Electronics, Inc. et al.*, Case No. 12-cv-00545-SLR (D. Del.). Served as an expert for Plaintiffs in a case alleging infringement of U.S. Patents 6,898,762, 7,065,709, 7,225,456, 7,493,643 and 8,112,776, relating to electronic television program guides. Case has settled. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304.

106. *Rovi Corporation et al. v. Vizio, Inc.*, Case No. 12-cv-00546-SLR (D. Del.). Served as an expert for Plaintiffs in a case alleging infringement of U.S. Patents 6,898,762, 7,065,709, 7,103,996 and 8,112,776, relating to electronic television program guides. Case has settled. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304.

107. *Rovi Corporation et al. v. Mitsubishi Electric Corp. et al.*, Case No. 12-cv-00547-SLR (D. Del.). Served as an expert for Plaintiffs in a case alleging infringement of U.S. Patents 6,701,523, 7,225,455 and 7,493,643, relating to electronic television program guides. Case has settled. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304.

108. *Netflix, Inc. v. Rovi Corporation et al.*, Case No. 11-cv-06591-PJH (N.D. Cal.). Served as an expert for Defendants in a declaratory judgment case seeking a declaration of non-infringement of U.S. Patents 6,305,016, 6,898,762, 7,100,185, 7,103,906 and 7,945,929, relating to electronic television program guides. Summary judgment was granted declaring all asserted claims invalid under 35 U.S.C. §101, affirmed by the Federal Circuit. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304. (R)

109. *Certain Products Containing Interactive Program Guide and Parental Control Technology*, USITC Inv. No. 337-TA-845. Served as an expert for Complainants Rovi Corporation et al. and against Netflix, Inc. et al. in an International Trade Commission proceeding involving alleged infringement of U.S. Patents 6,701,523, 6,898,762, 7,065,709, 7,103,906, 7,225,455, 7,493,643 and 8,112,776, relating to v-chips and electronic TV program guides. On Initial Determination, all claims Dr. Shamos testified about were found valid. The import requirement was found not satisfied and no infringement was found. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304. (D,R,T)

110. *Yardi Systems, Inc. v. Realpage, Inc. et al.*, Case No. 2:11-cv-0090-ODW-JEM (C.D. Cal.). Served as an expert for Defendants in an action alleging misappropriation of trade secrets, unfair competition, violation of the Computer Fraud and Abuse Act, the Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code §502) and the Digital Millennium Copyright Act, arising out of provision of cloud-based property management systems. Case has settled. Contact: Susan van Keulen, Esq., O'Melveny & Myers LLP, 2765 Sand Hill Road, Menlo Park, CA 94025.

111. *Long Range Systems, LLC v. HME Wireless, Inc.*, Civil Action 3:12-cv-03659-P (N.D. Tex.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patent 6,712,278, relating to a wireless system for locating a customer's table in a restaurant. Case was dismissed by plaintiff. Contact: David Cabello, Esq., Wong, Cabello, Lutsch, Rutherford & Brucculeri, LLP, 20333 SH 249, Suite 600, Houston, Texas 77070. (R)

112. *EdiSync Systems, LLC v. Centra Software, Inc. et al.*, Civil Action 03-cv-01587-WYD-MEH (D. Colo.). Served as an expert for Defendant Saba Software Inc. in a case alleging infringement of U.S. Patent 5,799,320, relating to multi-author document editing systems. Case has

settled. Contact: Robert M. Abrahamsen, Esq., Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210. (D,R)

113. *TecSec, Inc. v. IBM et al.*, Case No. 1:10-cv-115-LMB/TCB (E.D. Va.). Served as an expert for Defendant SAS Institute, Inc. in a case alleging infringement of U.S. Patents 5,369,702, 5,680,452, 5,717,755 and 5,898,781, relating to the Distributed Cryptographic Object Method, allowing embedding of encrypted objects within other objects. The Court entered judgment of non-infringement after Markman. Affirmed by the Federal Circuit at 2011-1303. Contact: Thomas R. Goots, Esq., Jones Day, North Point, 901 Lakeside Avenue, Cleveland, Ohio 44114-1190.

114. *Integrated Technological Systems, Inc. v. Green Dot Corporation*, Civ. Action No. 2:11-cv-01626-GMN-(GWF) (D. Nev.). Served as an expert for Defendant in a case alleging infringement of U.S. Patent 7,912,786, relating to an electronic payment system for transferring money between debit card accounts. Case has settled. Contact: Benjamin J. Sodey, Esq., Bryan Cave LLP, One Metropolitan Square (211 North Broadway), Suite 3600, St. Louis, MO 63102-2750.

115. *Hausen et al. v. PS Illinois Trust*, Case No. 11-cv-06888 (N.D. Ill.). Served as an expert for Plaintiff in a case concerning the reasonableness of credit card and email notification practices employed by a public storage facility prior to selling customers' stored goods. Case has settled. Contact: Jeffrey S. Becker, Esq., Swanson, Martin & Bell, LLP, 330 N. Wabash, Suite 3300, Chicago, IL 60611. (D,R)

116. *Linksmart Wireless Technology, LLC v. T-Mobile, USA, Inc. et al.*, Case 2:08-cv-264-DF-CE (E.D. Texas). Served as an expert for Defendant Choice Hotels International, Inc. in a case alleging infringement of U.S. Patent 6,779,118, relating to rule-based redirection of Internet service requests based on a user ID. Case has settled. Contact: Gregory R. Lyons, Esq., Wiley Rein LLP, 1776 K Street NW, Washington DC 20006.

117. *SAP America, Inc. v. Purple Leaf, LLC et al.*, Case No. 4:11-cv-04601-PJH (N.D. Cal.). Served as an expert for declaratory judgment plaintiff SAP in a case alleging infringement of U.S. Patents 7,603,311 and 8,027,913, relating to methods for conducting payment transactions over the Internet. Case has settled. Original firm: Simpson Thatcher & Bartlett LLP. Contact: Brian McCloskey, Esq., Greenberg Traurig, LLP, MetLife Building, 200 Park Ave., New York, NY 10166.

118. *Ameranth, Inc. v. PAR Technology Corp., et al.*, Civil Action 2-10-CV-294 JRG-RSP (E.D. Tex.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 6,384,850 and 6,871,325, relating to synchronous updating of hospitality applications and data on wireless devices. Case settled after expert reports were served. Contact: John W. Osborne, Esq., Osborne Law LLC, 33 Habitat Lane, Cortlandt Manor, NY 10567. (R)

119. *Digital-Vending Services International, LLC, v. The University of Phoenix, Inc. et al.*, Civil Action 2:09-cv-555-AWA-TEM (E.D. Va.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 6,170,014, 6,282,573 and 6,606,664, relating to content delivery

methods particularly applicable to online courseware. Summary judgment of non-infringement granted October 4, 2013. Contact: Andrew G. DiNovo, Esq., DiNovo Price Ellwanger & Hardy LLP, 7000 N. MoPac Expressway, Suite 350, Austin, TX 78731. (D,R)

120. *Analytical Mechanics Associates, Inc. v. Rhythm Engineering, LLC et al.*, Case No. 4:12-cv-00008 (E.D. Va.). Served as an expert for defendants in a case alleging breach of a contract relating to development of an image processing system to detect vehicles at intersections and control traffic signals. Case was resolved by binding arbitration. Contact: John K. Power, Esq., Husch Blackwell LLP, 4801 Main Street, Suite 1000, Kansas City, MO 64112. (D,R,T)

121. *Protegrity Corporation v. Voltage Security, Inc.*, Case No. 3:10-CV-755 (RNC) (D. Conn.). Served as an expert for defendant in a case alleging infringement of U.S. Patents 6,321,201, 6,963,980 and 7,325,129, relating to methods of encrypting databases. Case settled during trial. Contact: Edward G. Poplawski, Esq., Wilson Sonsini Goodrich & Rosati Professional Corporation, 650 Page Mill Road, Palo Alto, CA 94304-1050. (D,R,T)

122. *Progressive Casualty Insurance Company v. Allstate Insurance Company et al.,* Case No. 1:11-cv-00082-BYP (N.D.Ohio). Served as an expert for defendant Allstate in a case alleging infringement of U.S. Patent 6,064,970, relating to determining the cost of automobile insurance by monitoring the location and activity of a vehicle, and U.S. Patent 7,124,088, relating to online modification and quoting of insurance policies. Case has settled as to Allstate. Contact: James Medek, Esq., Kirkland & Ellis LLP, 300 North LaSalle Chicago, IL 60654.

123. *Symantec Corporation v. Acronis, Inc. et al.*, Case No. 3:11-cv-05310 EMC (N.D. Cal.). Served as an expert for plaintiff and infringement counterclaim defendant Symantec in a case alleging infringement of U.S. Patents 6,615,365, 7,047,380, 7,246,211 and 7,266,655, relating to online disk backup, imaging and recovery systems, U.S. Patent 7,093,086, relating to backup of virtual machines, U.S. Patent 7,322,010, relating to graphic views of computer configurations and U.S. Patent 7,565,517, relating to retargeting hardware configuration images to new hardware. Case has settled. Contact: Jennifer Kash, Esq., Quinn Emanuel Urquhart & Sullivan LLP, 50 California Street, 22nd Floor, San Francisco, California 94111. (D,R)

124. *Secure Axcess, LLC v. Bank of America Corp. et al.*, Civil Action No. 6:10-cv-670-LED (E.D. Tex.). Served as an expert for defendants Zions First National Bank and Amegy Bank N.A. in a case alleging infringement of U.S. Patent 7,631,191, relating to authenticating web pages. Case has settled as to those defendants. Contact: Brian Pandya, Esq., Wiley Rein LLP, 1776 K Street NW, Washington DC 20006.

125. *The MoneySuite Company v. Insurance Answer Center, LLC et al.,* Case No. SACV 11-1847-AG (C.D. Cal.). Served as an expert for defendants, including The Allstate Corporation, in a case alleging infringement of U.S. Patent 6,684,189, relating to online quoting of insurance policy rates. Case has settled. Contact: Garret A. Leach, Esq., Kirkland & Ellis LLP, 300 N. LaSalle, Chicago. IL 60654. (D,R)

126. *e-LYNXX Corporation v. Innerworkings, Inc. et al.*, CA 1:10-cv-02535-CCC (M.D. Pa.). Served as an expert for defendants, including R.R. Donnelley & Sons Company, in a case

alleging infringement of U.S. Patents 7,451,106 and 7,788,143, relating to electronic procurement of customized goods and services. The Court granted summary judgment of non-infringement in July 2013. Contact: James R. Nuttall, Esq., Steptoe & Johnson, LLP, 115 South LaSalle Street, Suite 3100, Chicago, IL 60603. (R)

127. *Vasudevan Software, Inc. v. Microstrategy, Inc.*, Case No. 3:11-cv-06637-RS-PSG (N.D. Cal.). Served as an expert for defendant in a case alleging infringement of U.S. Patents 6,877,006, 7,167,864, 7,720,861 and 8,082,268, relating to methods of online analytical processing (OLAP). The patents were found invalid on summary judgment. On appeal, the Federal Circuit upheld the Court's claim constructions and judgment of non-infringement. Declaratory judgment counterclaims voluntarily dismissed. Contact: Kevin A. Smith, Esq., Quinn Emanuel Urquhart & Sullivan, LLP, 50 California Street, San Francisco, CA 94111. (R)

128. *Digonex Technologies, Inc. v. Qcue, Inc.*, Case No. 1:12-cv-00801-SS (W.D. Texas). Served as an expert for plaintiff in a case alleging infringement of U.S Patents 8,095,424 and 8,112,303, relating to computerized methods for dynamic pricing. In a Markman order, the Court found the claims indefinite. Contact: David D. Schumann, Fenwick & West LLP, 555 California Street, 12th Floor, San Francisco, CA 94104. (D,R,T)

129. *Peter Mayer Publishers, Inc. v. Daria Shilovskaya et al.*, Case No. 12-CV-8867-PG (S.D. N.Y.). Served as an expert for declaratory judgment defendants in a case of first impression to determine whether a reliance party under 17 U.S.C. §104A(d)(3)(B) may issue an ebook version of a work to which copyright has been restored. The Court ruled that ebooks are not transformative and hence not derivative works. Contact: Timothy O'Donnell, Esq., 40 Exchange Place, 19th Fl., New York, NY 10005. (R)

130. *SIPCO, LLC v. Control4 Corporation et al.*, CA 1:11-cv-00612-JEC (N.D. Georgia). Served as an expert for defendants Schneider Electric Buildings Americas, Inc. and Schneider Electric USA, Inc. in a case alleging infringement of U.S. Patents 7,103,511, 7,468,661 and 7,697,492, relating to systems for monitoring remote sensors and controlling remote devices. Case has settled. Contact: Benjamin Bradford, Esq., Jenner & Block LLP, 353 N. Clark St., Chicago, IL 60654-3456.

131. *Unified Messaging Solutions LLC v. Google, Inc. et al.*, Case 1:12-cv-06286 (N.D. Ill.). Served as an expert for defendant eBay, Inc. in a case alleging infringement of U.S. Patents 6,857,074, 7,836,141, 7,895,306, 7,895,313, and 7,934,148, relating to message storage and delivery systems. Case has settled as to defendant eBay, Inc. Contact: Yar R. Chaikovsky, Esq., McDermott Will & Emery LLP, 275 Middlefield Road, Suite 100, Menlo Park, CA 94025.

132. *Credit Card Fraud Control Corporation v. PayPal, Inc.*, Case No. 9:12-CV-81143 (S.D. Fla.). Served as an expert for defendant PayPal in a case alleging infringement of U.S. Patent 8,229,844, relating to reduction of fraud in online transactions. Plaintiff dismissed the case with prejudice based on prior art located by PayPal. Contact: Adrian Percer, Esq., Weil, Gotshal & Manges, LLP, 201 Redwood Shores Parkway, Redwood Shores, CA 94065.

133. *Comscore, Inc. v. Integral Ad Science, Inc.*, Civil Action 2:12-cv-00351-HCM-DEM (E.D. Va.). Served as an expert for defendant Integral in a case alleging infringement of U.S. Patents 6,108,637, 6,115,680, 6,327,619, 6,418,470, 7,386,473, 7,613,635, 7,716,326 and 7,756,974, relating to determining whether a portion of a displayed page is visible to a user. Case has settled as to defendant Integral. Contact: Robert M. Abrahamsen, Esq., Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210.

134. *Ariba, Inc. v. Coupa Software, Inc.*, Case No. 3:12-cv-01484 JST (N.D. Cal.). Served as an expert for plaintiff Ariba in a case alleging infringement of U.S. Patent 7,117,165, relating to electronic methods for approving requisitions and generating purchase orders. Case has settled. Contact: Amy Van Zant, Esq., Covington & Burling LLP, 333 Twin Dolphin Drive, Redwood Shores, CA 94605-1418. (D,R)

135. *Lowe v. National Board for Respiratory Care, Inc. et al.*, Docket 1:12-cv-00345-DBH (D. Maine). Served as an expert for disabled plaintiff in a case seeking an injunction permitting to take a professional qualification examination using assistive computer technology. Case settled shortly after Dr. Shamos's declaration in support of preliminary injunction was filed. Contact: Kristin Aiello, Esq., Managing Attorney, Disability Rights Center, 24 Stone St., Augusta, ME 04338. (R)

136. *Checkfree Corporation et al. v. Metavante Corporation et al.*, Case No. 3:12-cv-15-J-34JBT (M.D. Fla.) Served as an expert for defendant Metavante in a case alleging infringement of U.S. Patents 7,383,223, 7,792,749, 7,853,524 and 7,966,311, relating to transferring funds in electronic payment networks. Defendants have counterclaimed, alleging infringement of U.S. Patents. 7,370,014, 7,734,543 and 7,958,049, relating to electronic invoice presentment. All claims of all four patents asserted by Plaintiff have been found invalid by the Patent Office. Case was stayed pending appeal, followed by voluntary dismissal by Plaintiff. Contact: Jeffrey A. Berkowitz, Esq., Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., Two Freedom Square, 11955 Freedom Drive, Reston, VA 20190-5675. (D,R)

137. *PPS Data, LLC v. Passport Health Communications, Inc.*, Case No. 2:12-cv-00438-DN (C.D. Utah). Served as an expert for defendant Passport in a case alleging infringement of U.S. Patents 6,341,265 and 7,194,416, relating to preparing and correcting health insurance claim forms. Case settled shortly after Dr. Shamos's claim construction report was served. Contact: Edward J. Pardon, Esq., Merchant & Gould, 10 East Doty Street, Suite 600, Madison, WI 53703. (R)

138. *Lodsys, LLC v. Combay, Inc. et al.*, Civil Action 2:11-cv-272 (E.D. Texas). Served as an expert for defendant Symantec Corporation in a case alleging infringement of U.S. Patents 7,222,078 and 7,620,565, relating to gathering feedback from products through a user interface. Case settled two weeks after Dr. Shamos's deposition. Contact: David D. Schumann, Fenwick & West LLP, 555 California Street, 12th Floor, San Francisco, CA 94104. (D,R)

139. *Long Range Systems, LLC v. HME Wireless, Inc.*, Civil Action 3:12-cv-04162M (N.D. Tex.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 6,542,751 and 7,062,281, relating to methods of paging customers at a restaurant. Case was dismissed by

plaintiff after a tentative Markman ruling. Contact: David Cabello, Esq., Wong, Cabello, Lutsch, Rutherford & Brucculeri, LLP, 20333 SH 249, Suite 600, Houston, Texas 77070. (R)

140. *Symantec Corporation v. Veeam Software Corporation*, Case No. 3:12-cv-0700-SI (N.D. Cal.). Served as an expert for plaintiff Symantec in a case alleging infringement of U.S. Patents 6,931,558, relating to methods for restoring network devices after failure, 7,024,527, relating to methods of backing up disk while applications are active, 7,093,086, relating to methods for backing up virtual machines, 7,254,682, relating to snapshot disk backup, 7,480,822, relating to restoring running states of computing systems, 7,831,861, relating to restoring application data and 8,117,168, relating to virtual disk backups. Case is stayed pending PTAB review. All asserted claims have been found unpatentable. On appeal to the Federal Circuit, the PTAB's claim construction and obviousness determinations were upheld, case remanded to allow amendment of claims. Case subsequently settled. Contact: Jennifer Kash, Esq., Quinn Emanuel Urquhart & Sullivan LLP, 50 California Street, 22nd Floor, San Francisco, California 94111. (R)

141. *EMG Technology, LLC v. Green Mountain Coffee Roasters and Keurig, Inc.*, Case No. 6:13-cv-144 (E.D. Texas) (Lead case: 6:13-cv-134). Served as an expert for Defendants in a case alleging infringement of U.S. Patent 7,441,196, relating to a method of navigating a Web page linked to a sister web site. Case has settled. Contact: Michael A. Albert, Esq., Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210.

142. *eDirect Publishing, Inc. v. Live Career, Ltd., et al.*, Case No. 12-CV-1123-JAH-JMA (S.D. Cal.). Served as an expert for plaintiff eDirect in a case alleging infringement of U.S. Patents 6,363,376 and 6,757,674, relating to automatic submission of information to career websites. Case has settled. Contact: Ryan Baker, Esq., Baker Marquart LLP, 10990 Wilshire Blvd., Los Angeles, CA 90024. (D,R)

143. *Motivation Innovations, LLC v. Ulta Salon Cosmetics and Fragrance, Inc. et al.*, C.A. No. 11-615-SLR-MPT (D. Del.). Served as an expert for defendant Ulta in a case alleging infringement of U.S. Patent 5,612,527, relating to a system for redeeming discount offers at point of sale. The Court granted summary judgment of noninfringement. Contact: Julie Heaney, Esq., Morris, Nichols, Arsht & Tunnell, LLP, 1201 North Market Street, Wilmington, DE 19899-1347. (D,R)

144. *Computer Software Protection, LLC v. Autodesk, Inc.*, C.A. No. 12-452-SLR (D. Del.). Served as an expert for Defendant Autodesk in a case alleging infringement of U.S. Patent 6,460,140, relating to unlocking the use of software remotely using validation number, a registration key and a license key. Case has settled. Contact: Cheryl T. Burgess, Esq., Knobbe, Martens, Olson & Bear, L.L.P., 2040 Main Street, 14th Floor Irvine, CA 92614. (R)

145. *Voltage Security, Inc.* v. *Protegrity Corporation*, CBM2014-0024, Patent Trial and Appeal Board. Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 8,402,281, relating to methods of encrypting databases. Matter has settled. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati Professional Corporation, 650 Page Mill Road, Palo Alto, CA 94304-1050. (R)

146. *United Video Properties, Inc. et al. v. Haier Group Corp. et al.*, C.A. No. 11-1140-KAJ (D.Del.). Served as an expert for Plaintiffs in a case alleging infringement of U.S. Patents 6,701,523 and 7,047,547, relating to television parental control technology. Case has settled. Contact: Hong S. Lin, Esq., Paul Hastings LLP, 1117 S. California Avenue, Palo Alto, CA 94304. (D,R)

147. *Droplets, Inc. v. E*TRADE Financial Corporation et al.*, Case No.: 1:12-CV-02326-CM (S.D.N.Y.). Served as an expert for defendants in an action alleging infringement of U.S. Patents 6,687,745 and 7,502,838, and 8,402,115, relating to delivering interactive links for presenting applications on a client computer. Defendants prevailed on a summary judgment of non-infringement on the '745 Patent. All claims of the '115 and '838 Patents were found invalid after IPRs, affirmed by the Federal Circuit in 2016-2504 and 2016-2602. Contact: Michael Levin, Esq., Wilson Sonsini Goodrich & Rosati Professional Corporation, 650 Page Mill Road, Palo Alto, CA 94304-1050. (D,R,T)

148. *Symantec Corporation v. Acronis, Inc. et al.*, Case No. 3:11-cv-05331 JST (N.D. Cal.). Served as an expert for plaintiff and infringement counterclaim defendant Symantec in a case alleging infringement by Symantec of U.S. Patents 7,366,859 and 7,831,789, relating to incremental disk backup, and infringement by Acronis of U.S. Patent 7,024,527, and 7,996,708, relating to disk backup and restore, U.S. Patent 7,454,592, and U.S. Patent 7,941,459, relating to single instance disk storage, and U.S. Patent 7,680,957, relating to modifiable representations of computer configurations. Case has settled. Contact: Jennifer Kash, Esq., Quinn Emanuel Urquhart & Sullivan LLP, 50 California Street, 22nd Floor, San Francisco, California 94111. (D,R)

149. *Jazz Pharmaceuticals, Inc. v. Roxane Laboratories, Inc.*, CA 2:10-cv-06108-ES-MCA (D. N.J.). Served as an expert for defendant in a case alleging infringement of U.S. Patents 7,668,730, 7,765,106, 7,765,107, 7,797,171 and 7,895,059, relating to methods of controlling the distribution of sensitive drugs. Case has settled. Contact: Alan B. Clement, Esq., Locke Lord LLP, Brookfield Place, 200 Vesey Street, 20th Floor, New York, NY 10281-2101. (R)

150. *TuitionFund, LLC v. SunTrust Banks, Inc. et al.*, CA 3:11-cv-00069 (M.D. Tenn.). Served as an expert for defendants Cardlytics, Inc., Regions Financial Corp., and Regions Bank in a case alleging infringement of U.S. Patents 7,499,872, 7,653,572 and 7,899,704, relating to methods for awarding rebates for credit and debit card purchases. Case settled. Contact: Michael S. Connor, Esq., Alston & Bird LLP, Bank of America Plaza, 101 South Tryon Street, Suite 4000, Charlotte, NC 28280-4000. (D,R)

151. *Pollin Patent Licensing, LLC et al. v. AT&T Corporation et al.*, Case No. 1:11-cv-07855 (N.D. Ill.). Served as an expert for defendants in a case alleging infringement of U.S. Patent 7,117,171, relating to verifying financial institution identification in electronic payment systems. Case has settled. Contact: James L. Howard, Esq., Kilpatrick Townsend & Stockton LLP, 1001 West Fourth Street Winston-Salem, NC, 27101.

152. *PPS Data, LLC v. Bluepoint Solutions, Inc.*, Case 2:13-cv-01351 (D. Nev.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 7,181,430, 7,216,106,

7,440,924, 7,624,071 and 8,126,809, relating to methods for processing check images in electronic payment systems. Case has settled. Contact: Anthony H. Son, Esq., Maddox Edwards, PLLC, 1900 K Street NW, Suite 725, Washington, DC 20006. (Original firm: Wiley Rein).

153. *e-LYNXX Corporation v. Ariba, Inc.*, CA 1:12-cv-01771-CCC (M.D. Pa.). Served as an expert for defendant Ariba, in a case alleging infringement of U.S. Patents 7,451,196, 7,788,143 and 8,209,227, relating to electronic procurement of customized goods and services. Case has settled. Contact: Amy Van Zant, Esq., Covington & Burling LLP, 333 Twin Dolphin Drive, Redwood Shores, CA 94605-1418.

154. *EMG Technology, LLC v. AutoZone, Inc.*, C.A. 6:13-cv-134 (E.D. Tex.) (Lead case: 6:12-cv-543). Served as an expert for defendant AutoZone in a case alleging infringement of U.S. Patent 7,441,196, relating to transcoding web sites into mobile sites. Defendant obtained summary judgment of non-infringement. Contact: Terry L. Clark, Esq., Bass, Berry & Sims PLC, 1201 Pennsylvania Ave. N.W., Washington, D.C. 20004. (R)

155. *In re: Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, on April 20, 2010,* MDL No. 2179 (E.D. La.). Served as an expert for litigants BP Exploration & Production Inc. et al. on an issue relating to identification of an anonymous person through Internet searching. Contact: Mark. J. Nomellini, Esq., Kirkland & Ellis LLP, 300 N. LaSalle, Chicago, IL 60654. (R)

156. *EC Data Systems, Inc., v. J2 Global, Inc. et al.*, CV 12-07544 (C.D. Cal.). Served as an expert for declaratory judgment plaintiff EC Data Systems in a case alleging infringement of U.S. Patents 6,208,638 and 6,350,066, 6,597,688 and 7,020,132, relating to electronic distribution of faxes through email. Case has settled. Contact: Matthew Spohn, Esq. Norton Rose Fulbright LLP., Tabor Center, 1200 17th Street, Suite 1000, Denver, Colorado 80202.

157. *MoneyCat, Ltd. v. PayPal, Inc.*, CA 1:13-cv-01358-RGA (D. Del.), now 3:14-cv-02490-PSG (N.D. Cal.). Served as an expert for defendant PayPal in a case alleging infringement of U.S. Patents 7,590,602, 8,195,578 and 8,051,011, relating to issuance and transfer of electronic currency. On CBM review, the PTAB found all asserted claims of all three patents invalid, affirmed by the Federal Circuit. Case was subsequently dismissed. Contact: Adrian Percer, Esq., Weil, Gotshal & Manges, LLP, 201 Redwood Shores Parkway, Redwood Shores, CA 94065. (D,R)

158. *GSI Commerce Solutions, Inc.* v. *Clear With Computers, Inc.*, Patent Trial and Appeal Board Case CBM2013-00055. Served as an expert for petitioner, an eBay company, in a covered business method review of U.S. Patent 8,266,015, relating to methods of presenting lists of product customization options. Review was instituted but the CBM was terminated by settlement. Contact: Scott McKeown, Esq., Ropes & Gray, L.L.P., 2099 Pennsylvania Avenue, Washington, DC 20006-6807. (D,R)

159. *Fidelity National Information Services, Inc. v. Cashedge, Inc. and Checkfree Corporation*, Patent Trial and Appeal Board Cases CBM2013-00028, 30, 31 and 32. Served as

an expert for petitioner in covered business method reviews of U.S. Patents 7,383,223, 7,792,749, 7,853,524 and 7,966,311, relating to transferring funds in electronic payment networks. Reviews have been instituted. All claims of the four patents were invalidated by the PTAB in December 2014. Appeal was taken to the Federal Circuit but terminated by agreement. Contact: Jeffrey A. Berkowitz, Esq., Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., Two Freedom Square, 11955 Freedom Drive, Reston, VA 20190-5675. (D,R)

160. *Boku, Inc. v. Xilidev, Inc.*, Patent Trial and Appeal Board Cases CBM2014-00140 and CBM2014-00148. Served as an expert for petitioner in two covered business method reviews of U.S. Patent 7,273,168, relating to authorizing payments via handheld devices. Result: claims 1-18 and 20-23 found invalid. Claim 19 cancelled. Contact: Frank Pietrantonio, Esq., Cooley LLP, One Freedom Square, 11951 Freedom Drive, Reston, VA 20190. (R)

161. *Protegrity Corporation v. Phoenix Payment Systems, Inc. d/b/a Electronic Payment Exchange*, Case No. 3:13-CV-1386-VKB (D. Conn.). Served as an expert for defendant in a case alleging infringement of U.S. Patents 6,321,201 and 8,402,281, relating to methods of encrypting databases. Case has settled. Contact: David J. Wolfsohn, Esq., Duane Morris LLP, 20 South 17th Street, Philadelphia, PA 19103. (R)

162. *Ameranth, Inc. v. Genesis Gaming Solutions, Inc. et al.*, Case No. SACV 8:11-0189-AG (C.D. Cal.). Served as an expert for Ameranth in a case alleging infringement of U.S. Patents 7,431,650, 7,878,909 and 8,393,969, relating to systems for managing casino operations, particularly in poker rooms. Case has settled. Contact: John W. Osborne, Esq., Osborne Law LLC, 33 Habitat Lane, Cortlandt Manor, NY 10567. (D,R)

163. *Telebuyer, LLC v. Amazon.com, Inc.*, Case No. 2:13-cv-01677-BJR (W.D. Wash.). Served as an expert for Telebuyer in a case alleging infringement by Amazon.com of U.S. Patents 6,323,894, 7,835,508, 7,835,509, 7,839,984, 8,059,796, 8,098,272, and 8,315,364, relating to systems for interfacing buyers and sellers via communication networks. Summary judgment was entered declaring all asserted claims invalid under 35 U.S. §101. Contact: Brian Berliner, Esq., O'Melveny & Myers LLP, 400 South Hope Street, Los Angeles, CA 90071. (D,R)

164. *GlobeRanger Corporation v. Software AG, et al.*, Civil Action No. 3:11-CV-403-B (N.D. Texas). Served as an expert for GlobeRanger in a case alleging misappropriation of trade secrets and civil conspiracy involving radio-frequency identification (RFID) software and business processes. Result: jury verdict of $15 million in favor of GlobeRanger, upheld on appeal to the Fifth Circuit. Contact: Ophelia Camiña, Esq., Susman Godfrey, L.L.P., 901 Main St., Suite 5100, Dallas, TX 75202-3775. (D,R,T)

165. *In re: ProvideRx of Grapevine, LLC and CERx Pharmacy Partners, LP v. Provider Meds, LP, et al.*, Adv. Proc. No. 13-03015-BJH (Bankr. N.D. Tex). Served as an expert for creditor CERx in a Chapter 7 bankruptcy case involving security interests in software for remote dispensing pharmacies and whether certain licenses constitute encumbrances under Texas law. Case has settled. Contact: Bill Whitehill, Esq., Gardere Wynne Sewell LLP, 1601 Elm St., Dallas, TX 75201. (R)

166. *Square, Inc. v. Protegrity Corporation*, CBM2014-00182, Patent Trial and Appeal Board (2014). Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 8,402,281, relating to methods of encrypting databases. Result: all claims invalid under §101. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati Professional Corporation, 650 Page Mill Road, Palo Alto, CA 94304-1050. (D,R)

167. *VigLink, Inc. v. Linkgine, Inc.*, Patent Trial and Appeal Board (2014). Served as an expert for petitioner in covered business method petitions 2014-00184 and 2014-00185 seeking review of U.S. Patents 7,818,214 and 8,027,883, relating to modifying affiliate links on webpages. Result: all challenged claims found invalid. Affirmed by the Federal Circuit at 2016-2087, 2016-2088. Contact: Robert C. Hilton, Esq., McGuireWoods LLP, 2000 McKinney Ave., Suite 1400, Dallas, TX 75201. (R)

168. *Juhline et al. v. Ben Bridge Jewelers Inc. et al.*, Case 11-cv-2096-GPC-NLS (S.D. Cal.). Served as an expert for defendant Ben Bridge in a class action alleging violation of California Civil Code §1747.8, relating to the collection of personal identification information in connection with credit card transactions. Case has settled. Contact: Rosemarie T. Ring, Esq., Munger, Tolles & Olson LLP, 560 Mission St., 27th Fl., San Francisco, CA 94105.

169. *Catch Curve, Inc. v. Integrated Global Concepts, Inc. v. j2 Global Communications, Inc. et al.*, Case 1:06-CV-02199 (N.D. Ga.). Served as an expert for defendant and counterclaim plaintiff Integrated Global Concepts in a case alleging infringement of U.S. Patents 4,994,926, 5,291,302, 5,459,584, 6,643,034, 6,785,021, 7,365,884 and 7,525,691, relating to store-and-forward fax systems. Infringement claims were dropped. The issue at bar is whether j2 Global had an objective basis to believe that Integrated Global was infringing. Case has settled. Contact: James Heiser, Esq., Chapman and Cutler, LLP, 111 West Monroe St., Chicago, IL 60603. (D,R)

170. *Phoenix Payment Systems, Inc. v. Protegrity Corporation*, CBM2014-00121, Patent Trial and Appeal Board (2014). Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 8,402,281, relating to methods of encrypting databases. Underlying litigation settled before CBM could be instituted. Contact: Contact: David J. Wolfsohn, Esq., Duane Morris LLP, 20 South 17th Street, Philadelphia, PA 19103. (R)

171. *Informatica Corporation v. Protegrity Corporation*, CBM2015-00010, CBM2015-00021, Patent Trial and Appeal Board (2014). Served as an expert for petitioner in two covered business method petitions seeking review of U.S. Patents 8,402,281 and 6,321,201, relating to methods of encrypting databases. Result: all claims found invalid under 35 U.S.C. §101. The Board's opinions in the '201 case and the '281 case comment favorably on Dr. Shamos's testimony. Contact: Mark S. Kaufman, Esq., Reed Smith LLP, 1301 K Street N.W., Washington, DC 20005. (D,R)

172. *Qualtrics, LLC v. OpinionLab, Inc.*, IPR2014-00314, IPR2014-00356, IPR2014-00366, IPR2014-00406, IPR2014-00420, and IPR2014-00421, Patent Trial and Appeal Board (2014). Served as an expert for patent owner OpinionLab, Inc. in *inter partes* reviews of U.S. Patents 6,421,724, 6,606,581, 8,041,805, 7,085,820, 7,370,285 and 8,024,668, relating to

methods of soliciting page-specific feedback regarding web pages. All challenged claims have been found invalid except as to the '805 patent. '724 was not instituted. Contact: Chris Kennerly, Esq., Paul Hastings LLP, 1117 S. California Ave., Palo Alto, CA 94304. (D,R)

173. *Callwave Communications, LLC v. AT&T Mobility, LLC et al.*, Case 1:12-cv-01788-RGA (D. Del.). Served as an expert for defendant Research In Motion, Corp. in a case alleging infringement of U.S. Patent 7,907,933, relating to methods of billing for purchases by placing a call to a pay-per-call service. Plaintiff stipulated to non-infringement for appeal purposes, but the Federal Circuit upheld on January 10, 2017. Contact: John V. Gorman, Esq., Morgan, Lewis & Bockius LLP, 1701 Market Street, Philadelphia, PA 19103.

174. *SoftVault Systems, Inc. v. Dassault Systèmes Solidworks Corporation*, Case 5:14-cv-03221-LHK (N.D. Cal.). Served as an expert for defendant Solidworks. in a case alleging infringement of U.S. Patents 6,249,868 and 6,594,765 relating to embedded agents for protecting computer systems against theft. Case has settled. Contact: Cheryl T. Burgess, Esq., Knobbe, Martens, Olson & Bear, L.L.P., 2040 Main Street, 14th Floor Irvine, CA 92614.

175. *PPS Data, LLC v. TransCentra, Inc.*, Case 13-359-LPS (D. Del.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 7,181,430, 7,440,924, 7,624,071 and 8,126,809, relating to methods for processing check images in electronic payment systems. Case has settled. Contact: Anthony H. Son, Esq., Maddox Edwards, PLLC, 1900 K Street NW, Suite 725, Washington, DC 20006. (Original firm: Wiley Rein).

176. *Clear With Computers, Inc. v. Spanx, Inc.*, C.A. 6:12-cv-950-LED (E.D. Texas). Served as an expert for defendant, an eBay company, in a case alleging infringement of U.S. Patent 8,266,015, relating to methods of presenting lists of product customization options. Judgment on the pleadings was granted, invalidating the asserted claims under 35 U.S.C. §101. Case was appealed to the Federal Circuit, but the appeal with withdrawn. Case has settled. Contact: Scott McKeown, Esq., Oblon, Spivak, McClelland, Maier & Neustadt, L.L.P., 1940 Duke Street Underpass, Alexandria, VA 22314.

177. *Integrated Global Concepts, Inc. v. Advanced Messaging Technologies, Inc.*, IPR2014-01027 and IPR2014-01028 Patent Trial and Appeal Board (2014). Served as an expert for petitioner seeking *inter partes* review of U.S. Patents 6,020,980, relating to delivering faxes through electronic mail. The PTAB declined to institute review. Contact: Robert J. Schneider, Esq., Taft Stettinius & Hollister LLP, 111 East Wacker, Suite 2800, Chicago, IL 60601. (R)

178. *athenahealth, Inc. v. AdvancedMD Software, Inc.*, Civil Action 1:11-cv-11260-GAO (D. Mass.). Served as an expert for plaintiff athenahealth, Inc. in a case alleging infringement of U.S. Patents 7,617,116 and 7,720,701, relating to detecting errors in medical insurance claim submissions and automated configuration of medical practice management systems. Case has settled. Contact: Robert M. Abrahamsen, Esq., Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210.

179. *CEATS, Inc. v. Orbitz Worldwide, Inc.*, Civil Action 2:13-cv-01385-MMD-PAL (D. Nev.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents

7,548,667, 7,640,178, 7,660,727, 8,219,448, 8,229,774 and 8,244,561, relating to systems and methods for managing airline seat reservations. Case has settled. Contact: Jared Bunker, Esq., Knobbe, Martens, Olson & Bear, L.L.P., 2040 Main Street, 14th Floor Irvine, CA 92614.

180. *Audatex North America, Inc. v. Mitchell International, Inc.*, Civil Action 3:13-cv-01523-BEN (BLM) (S.D. Cal.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 7,912,740, 8,200,513 and 8,468,038, relating to systems and methods for determining the valuation of a damaged vehicle for insurance purposes. Claims found invalid after CBM review, affirmed by the Federal Circuit. Contact: David McPhie, Esq., Irell & Manella LLP, 840 Newport Center Dr., Newport Beach, CA 29660. (R)

181. *Skimlinks, Inc. et al. v. Linkgine, Inc.*, Patent Trial and Appeal Board (2015). Served as an expert for petitioners in covered business method petitions 2015-00086 and 2015-00087 seeking review of U.S. Patents 7,818,214 and 8,027,883, relating to modifying affiliate links on webpages. Result: all claims found invalid, affirmed by the Federal Circuit. Contact: Richard F. Martinelli, Esq., Orrick, Herrington & Sutcliffe LLP, 51 West 52nd St., New York, NY 10019. (R)

182. *Advanced Auctions, LLC. v. eBay, Inc.*, Case 12-cv-1612-BEN (JLB) (S.D. Cal.). Served as an expert for defendant eBay in case alleging infringement of U.S. Patent 8,266,000, relating to methods of conducting Internet auctions. Defendant obtained judgment of invalidity on the pleadings under 35 U.S.C. §101. Contact: Adrian Percer, Esq., Weil, Gotshal & Manges, LLP, 201 Redwood Shores Parkway, Redwood Shores, CA 94065.

183. *MaxMind, Inc. et al. v. Fraud Control Systems.com Corporation*, CBM2015-00094, Patent Trial and Appeal Board (2014). Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 8,630,942, relating to methods of determining whether a payment transaction may be fraudulent based on IP addresses. Review was instituted on §101 grounds and Patent Owner requested adverse judgment. Contact: Anthony H. Son, Esq., Maddox Edwards, PLLC, 1900 K Street NW, Suite 725, Washington, DC 20006. (R)

184. *Square, Inc. v. Unwired Planet, LLC*, CBM2014-00156, Patent Trial and Appeal Board (2014). Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 7,711,100, relating to conducting point-of-sale transactions based on the location of a wireless device. Challenged claims found invalid. Contact: Sasha G. Rao, Esq., Maynard Cooper and Gale PC, 275 Battery St., San Francisco, CA 94111 (D,R)

185. *Unified Patents, Inc. v. Finnavations LLC*, IPR2015-01209, Patent Trial and Appeal Board (2015). Served as an expert for petitioner in an inter partes review of U.S. Patent 8,132,720, relating to verifying online transaction data through a graphical user interface. Status: not instituted. Contact: Paul C. Haughey, Esq., Kilpatrick Townsend & Stockton LLP, Eighth Floor, Two Embarcadero Center San Francisco, CA 94111 (R)

186. *Hoskin Hogan et al. v. BP West Coast Products LLC et al.*, Case BC 460880 (Super. Ct. Los Angeles Cty. CA, 2011). Served as an expert for defendant Retalix Ltd., alleging negligence in the development and testing of software for processing point-of-sale transactions. Summary

judgment granted in favor of Retalix. Contact: Richard H. Zelichov, Esq., Katten Muchin Rosenman LLP, 2029 Century Park East, Suite 2600, Los Angeles, CA 90067-3012. (D,R)

187. *In re U.S. Patent Application 12/912,726* (USPTO). Served as an expert for applicant AlmondNet, Inc. in an application for a patent relating to distributing digital advertising based on a recipient profile. PTAB affirmed the Examiner's § 101 rejection. Contact: Louis J. Hoffman, Esq., Hoffman Patent Firm. (R)

188. *Wickfire, LLC v. TriMax Media, Inc. et al.*, C.A. 1:14-CV-34 (W.D. Tex). Served as an expert for defendants in a case alleging click fraud in Internet advertising. Jury verdict for Plaintiff, reversed on appeal to the Fifth Circuit. Contact: Barry M. Golden, Esq., Miller, Egan, Molter & Nelson LLP, 2911 Turtle Creek Blvd., Suite 1100 Dallas, TX 75219. (D,R,T)

189. *Square, Inc. v. Unwired Planet, LLC*, CBM2015-00148, Patent Trial and Appeal Board. Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 7,711,100, relating to conducting point-of-sale transactions based on the location of a wireless device. Not instituted because claims were found invalid under § 101 in CBM2014-00156. Contact: Sasha G. Rao, Esq., Maynard Cooper and Gale PC, 275 Battery St., San Francisco, CA 94111. (D,R)

190. *Datatrak International Inc. v. Medidata Solutions, Inc.*, C.A. 1:11-cv-00458-PAG (N.D. Ohio). Served as an expert for defendant in a case alleging infringement of U.S. Patent 7,464,087, relating to federated database queries. Defendant obtained summary judgment of invalidity under 35 U.S.C. §101. Contact: Duane-David Hough, Esq., Mayer Brown LLP, 1675 Broadway, New York, NY 10019. (R)

191. *SNMP Research, Inc. et al. v. Avaya, Inc.*, C.A. 1:12-cv-00191-RGA-MPT (D. Del.). Served as an expert for Avaya in an action alleging breach of contract, trade secret misappropriation and copyright infringement involving software implementing the Simple Network Management Protocol (SNMP). Case has settled. Contact: Joshua Krumholz, Esq., Holland & Knight, LLP, 10 St. James Avenue, 11th Floor, Boston, MA 02116. (D,R)

192. *Certain Automated Teller Machines and Point of Sale Devices and Associated Software Therefor*, USITC Inv. No. 337-TA-958. Served as an expert for Respondents NRT Technology Corp. et al. in an International Trade Commission proceeding brought by Complainant Global Cash Access Inc. involving alleged infringement of U.S. Patent 6,081,792, relating to structuring ATM and POS transactions with respect to withdrawal limits. Result: all claims found invalid as indefinite. In affirming this determination, the Commission wrote: "should the extrinsic evidence be considered, the Commission finds NRT's expert testimony credible, see Rebuttal Expert Report of Michael Shamos Regarding Claim Construction ¶¶ 52-58, and that Everi's expert's testimony is not credible." Contact: Colby B. Springer, Esq., Polsinelli LLP (formerly at Lewis Roca Rothgerber LLP), Three Embarcadero Center, Suite 1350, San Francisco, CA 94111. (D,R)

193. *Better Mouse Company, L.L.C. v. SteelSeries ApS, Inc. et al.*, C.A. 2:14-cv-198-JRG (E.D. Texas). Served as an expert for defendant in a case alleging infringement of U.S. Patent

7,532,200, relating to computer mouse whose resolution can be set without external software. Dr. Shamos testified at trial on non-infringement. The jury found for defendant on non-infringement. Contact: Joshua M. Masur, Esq., Zuber Lawler & Del Duca LLP, 2000 Broadway, Suite 154, Redwood City, California 94063. (Original firm: Turner Boyd LLP) (R,T)

194. *Vesta Corporation v. Amdocs Management Limited et al.*, No. 3:14-cv-01142-HZ (D. Ore.). Served as an expert for defendants in a case alleging misappropriation of trade secrets relating to billing in the prepaid mobile phone payment processing market. Case has settled. Contact: Yonaton M. Rosenzweig, Esq., Katten Muchin Rosenman LLP, 2029 Century Park East, Suite 2600, Los Angeles, CA 90067-3012. (D,R)

195. *Benefit Funding Systems, LLC et al. v. U.S. Bancorp*, CA 1:12-cv-00803-LPS (D.Del.). Served as an expert for defendant U.S. Bancorp in an action alleging infringement of U.S Patent 6,625,582, relating to a method of establishing a financial account based on the present value of future retirement payments. All asserted claims were found invalid under 35 U.S.C. §101, a decision affirmed by the Federal Circuit. Contact: Contact: Anthony H. Son, Esq., Maddox Edwards, PLLC, 1900 K Street NW, Suite 725, Washington, DC 20006. (Original firm: Wiley Rein).

196. *Telesign Corporation v. Twilio, Inc.*, C.A. 3:18-cv-03279-VC (N.D. Cal.). Served as an expert for defendant Twilio in an action alleging infringement of U.S. Patent 7,945,034, relating to verification of telephone users based on characteristics of the telephone number, such as carrier and geographic location. Defendant successfully resisted issuance of a preliminary injunction. Case is stayed pending PTAB review. After PTAB review, Twilio's motion for judgment on the pleadings was granted. Contact: Thomas J. Friel, Jr., Esq., Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. (R)

197. *Cronos Technologies, LLC v. Expedia, Inc.*, C.A. 13-1538-LPS (D. Del.), *Cronos Technologies, LLC v. Priceline.com, Inc.*, C.A. 13-1541-LPS (D. Del.) and *Cronos Technologies, LLC v. Travelocity.com L.P.*, C.A. 13-1544-LPS (D. Del.). Served as an expert for defendants in three cases, consolidated for some purposes, in actions alleging infringement of U.S. Patent 5,664,110, relating to a remote ordering system enabling a user to build lists of products to be ordered. The Court found non-infringement on summary judgment, affirmed unanimously by the Federal Circuit. Contact: Matthew C. Acosta, Esq., Jackson Walker LLP, KPMG Plaza at Hall Arts, 2323 Ross Avenue, Suite 600, Dallas, TX 75201. (D,R)

198. *Ex Parte Reexamination of U.S. Patent 7,333,430*, Control No. 90/013,532. Served as an expert for patent owner Fortinet, Inc. in a reexamination of U.S. Patent 7,333,430, drawn to distributing network packets for intermediate security processing based on the ultimate destination of the packet. Result: all challenged claims and newly presented claims patentable. Contact: Michael A. DeSanctis, Hamilton DeSanctis & Cha LLP, Financial Plaza at Union Square, 225 Union Boulevard, Ste. 150, Lakewood, CO 80228. (R)

199. *ServiceNow, Inc. v. Hewlett-Packard Company,* Case IPR2015-00717 (PTAB). Served as an expert for patent owner Hewlett-Packard Company in an inter partes review of U.S. Patent 7,027,411, drawn to efficient determination of changes in network topology. Status: settled.

Contact: Monica Grewal, Esq., Wilmer Cutler Pickering Hall and Dorr LLP, 60 State Street, Boston, MA 02109. (D,R)

200. *Intellectual Ventures I LLC v. Nextel Operations, Inc. and Sprint Spectrum L.P.*, C.A. No. 13-1634 (D.Del) and related cases 13-1635; *Intellectual Ventures I LLC v. T-Mobile USA, Inc. et al.*, C.A. No. 13-1632; 13-1633; *Intellectual Ventures I LLC v. United States Cellular Corporation*, C.A. No. 13-1636 and related case 13-1637, all D. Del. Served as an expert for defendants Sprint, T-Mobile and U.S. Cellular in related cases alleging infringement of U.S. Patent 6,115,737, drawn to use of an Internet gateway for processing customer service requests to a web server. The Court invalidated the '737 patent on §101 grounds. Contact: Jason W. Cook, Esq., McGuireWoods LLP, 2000 McKinney Ave., Suite 1400, Dallas, TX 75201. (D,R)

201. *Ex Parte Reexamination of U.S. Patent 7,968,744*, Control No. 90/013,533. Served as an expert for patent owner Fortinet, Inc. in a reexamination of U.S. Patent 7,968,744, drawn to systems and methods for allowing execution of authorized computer code and for protecting computer systems and networks from unauthorized code execution. Result: challenged claim and 14 new claims determined patentable. Contact: Michael A. DeSanctis, Hamilton DeSanctis & Cha LLP, Financial Plaza at Union Square, 225 Union Boulevard, Ste. 150, Lakewood, CO 80228. (R)

202. *Ex Parte Reexamination of U.S. Patent 7,376,125*, Control No. 90/013,531. Served as an expert for patent owner Fortinet, Inc. in a reexamination of U.S. Patent 7,376,125, drawn to a virtual routing engine for software-based packet routing. Result: newly presented claims patentable. Contact: Michael A. DeSanctis, Hamilton DeSanctis & Cha LLP, Financial Plaza at Union Square, 225 Union Boulevard, Ste. 150, Lakewood, CO 80228. (R)

203. *Twilio, Inc. v. Telesign Corporation*, IPR2016-00360. Served as an expert for requester Twilio in an *inter partes* review of U.S. Patent 7,945,034, relating to verification of telephone users based on characteristics of the telephone number, such as carrier and geographic location. Challenged claims confirmed. Contact: Thomas J. Friel, Jr., Esq., Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. (D,R)

204. *Twilio, Inc. v. Telesign Corporation*, IPR2016-00450, Patent Trial and Appeal Board (2016). Served as an expert for petitioner in an *inter partes* review of U.S. Patent 8,462,920, relating to verification of telephone users based on characteristics of the telephone number, such as carrier and geographic location. Trial was not instituted. Contact: Contact: Carrie J. Richie, Esq., Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. (R)

205. *Smart Systems Innovations, LLC v. Chicago Transit Authority, et al.*, C.A. 14-cv-08053 (N.D. Ill.). Served as an expert for defendants in an action alleging infringement of U.S. Patent 5,828,044, relating to a radio-frequency ID (RFID) credit card system. Defendant successfully resisted issuance of a preliminary injunction. All claims invalidated as non-statutory under 35 U.S.C. §101. Affirmed by the Federal Circuit in October 2017. Contact: Jeffrey M. Connor., Esq., formerly at Kilpatrick Townsend & Stockton LLP, now IP counsel at Honeywell. (D,R)

206. *Unwired Planet LLC v. Google, LLC*, C.A. 3:12-cv-00504-MMD-VPC (D. Nevada). Served as an expert for Google in an action alleging infringement of U.S. Patents 6,292,657, 6,654,786, 6,662,016, 6,684,087, 6,895,240, 6,944,760, 7,024,205, 7,035,647, 7,203,752 and 7,463,151, relating to provision of wireless services. All asserted claims of the '151, '205 and '751 patents have been found invalid by the Patent Trial and Appeal Board. After appeal to the Federal Circuit, the case continued with respect to certain claims of the '752 Patent but these were dismissed by stipulation. Contact: Peter E. Gratzinger, Esq., Munger, Tolles & Olson LLP, 355 South Grand Avenue, Los Angeles, CA 90071.

207. *Xilidev, Inc. v. Boku, Inc. et al.*, C.A. 3:13-cv-02793 (S.D. Cal.). Served as an expert for defendants in an action alleging infringement of U.S. Patent 7,273,168, relating to point-of-sale billing on handheld devices. Claims 1-18 and 20-23 of the '168 patent have been found invalid by the Patent Trial and Appeal Board. Plaintiff agreed to a voluntary dismissal with prejudice. Contact: Frank Pietrantonio, Esq., Cooley LLP, One Freedom Square, 11951 Freedom Drive, Reston, VA 20190.

208. *Intellectual Ventures II LLC v. Commerce Bancshares, Inc. et al.*, C.A. 2:13-CV-04160 (W.D. Mo.). Served as an expert for defendants in an action alleging infringement of U.S. Patents 5,745,574, relating to security in electronic transactions, 6,314,409 and 6,826,694, relating to controlling access to digital property, 6,715,084, relating to intrusion detection, and 7,634,666, relating to a cryptographic engine. All asserted claims have been declared invalid by the Patent Trial and Appeal Board. Decision affirmed by the Federal Circuit in December 2016. Contact: Mark Vander Tuig, Esq., Senniger Powers LLP, 100 North Broadway, 17th Floor, St. Louis, MO 63102.

209. *Hy-Vee, Inc. v. Inmar Digital Promotions Network, Inc.*, C.A. 4:15-cv-00275 (S.D. Iowa). Served as an expert for defendant in an action seeking indemnity for infringement of U.S. Patents 8,219,445, 8,370,199 and 8,538,805, relating to point-of-sale processing of promotions, such as coupons. Hy-Vee had been sued for infringing these patents in *Advanced Marketing Systems, LLC v. Hy-Vee, Inc.*, C.A. 3:15-cv-00103 (W.D. Wisc.). Both cases have settled. Contact: Richard J. Keshian, Esq., Kilpatrick Townsend & Stockton LLP, 1001 West Fourth Street Winston-Salem, NC, 27101. (R)

210. *Motivation Innovations, LLC v. PetSmart, Inc.*, C.A. 1:13-cv-00957 (D.Del.). Served as an expert for defendant in an action alleging infringement of U.S. Patent 5,612,527, relating to a system for redeeming discount offers at point of sale. On motion for judgment on the pleadings, all asserted claims were found invalid under 35 U.S.C. §101. Contact: Kevin A. Zeck, Esq., Perkins Coie, LLP, 1201 Third Avenue, Suite 4900, Seattle, WA 98101-3099.

211. *PPS Data, LLC v. VSoft Corporation et al.*, Case 1:15-cv-00084 (N.D. Ga.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 7,181,430, 7,216,106, 7,440,924, 7,624,071 and 8,660,956, relating to methods for processing check images in electronic payment systems. Case has settled. Contact: Anthony H. Son, Esq., Maddox Edwards, PLLC, 1900 K Street NW, Suite 725, Washington, DC 20006 (original firm Andrews Kurth).

212. *Sally Beauty Holdings et al. v. Intellectual Ventures I LLC*, CBM2016-00029, Patent Trial and Appeal Board. Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 5,969,324, relating to accounting methods utilizing a non-predictable bar code. Trial was instituted, the PTAB writing in its decision: "We credit the testimony of Dr. Michael Shamos." Case has settled. Contact: Derek Swanson, Esq., McGuireWoods LLP, Gateway Plaza, 800 East Canal Street, Richmond, VA 23219. (R)

213. *Square, Inc. v. Protegrity Corporation*, CBM2015-00014, Patent Trial and Appeal Board (2016). Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 6,321,201, relating to methods of encrypting databases. Result: all challenged claims found invalid under 35 U.S. §§101 and 103. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati Professional Corporation, 650 Page Mill Road, Palo Alto, CA 94304-1050. (R)

214. *T-Mobile US, Inc. v. Intellectual Ventures II LLC*, CBM2016-00083, Patent Trial and Appeal Board. Served as an expert for petitioner in a covered business method petition seeking review of U.S. Patent 6,115,737, relating to use of an Internet gateway for processing customer service requests to a web server. The PTAB determined that the patent did not claim a covered business method. Contact: Alison R. Watkins, Esq., Gibson, Dunn & Crutcher LLP, 1881 Page Mill Road, Palo Alto, CA 94304-1211. (R)

215. *Twin Peaks Software, Inc. v. IBM Corporation*, Case 3:14-cv-03933-JST (N.D. Cal.). Served as an expert witness for defendant IBM in an action alleging infringement of U.S. Patent 7,418,439, relating to a system for storing and sharing networked files. All asserted claims found invalid during claim construction. Contact: Andrew Bramhall, Esq., Quinn Emanuel Urquhart & Sullivan, LLP, 555 Twin Dolphin Drive, 5th Floor, Redwood Shores, CA 94065-2139.

216. *Live Face on Web, LLC v. The Control Group Media Company, Inc. et al.*, Case 2:15-cv-01306 (E.D. Pa.). Served as an expert witness for defendants in an action alleging breach of contract and infringement of copyrights relating to web media players and video productions in which recorded actors promote products for websites. Case has settled. Contact: Damon W.D. Wright, Esq., Venable LLP, 575 Seventh St. N.W., Washington, DC 20004.

217. *Nomadix, Inc. v. Hospitality Core Services, LLC*, Case 2:14-cv-08256-DDP (C.D. Cal.) Served as an expert witness for defendant in a case alleging infringement of U.S. Patents 6,636,894 and 6,868,399, relating to network gateways, U.S. Patent 7,698,432, relating to bandwidth management, U.S. Patent 7,953,857, relating to dynamic data transfer over networks, U.S. Patent 8,266,266, relating to dynamic network authorization, and U.S. Patents 8,156,246, 8,266,269, 8,364,806, 8,725,888 and 8,788,690, relating to providing network content. Case has settled. Contact: Michael J. Mehrman, Merhman Law Office, P.C., 150 Spalding Creek Court, Sandy Springs, GA 30350.

218. *Certain Digital Video Receivers and Hardware and Software Components Thereof*, USITC Inv. No. 337-TA-1001. Served as an expert for Complainants Rovi Corporation et al. against Comcast Corporation et al. in an International Trade Commission proceeding involving alleged infringement of U.S. Patents 8,006,263 , 8,046,801 and 8,578,413, relating to remote

and local electronic TV program guides. On Final Determination, a violation was found with respect to the '263 and '413 patents. Affirmed by the Federal Circuit on March 20, 2020. Contact: Richard A. Kamprath, Esq., McKool Smith, 300 Crescent Court, Suite 1500, Dallas, TX 75201. (D,R,T)

219. *ZKey Investments, LLC v. Facebook, Inc.,* Case 2:16-cv-00782-RSWL-KS (C.D. Cal.). Served as an expert for defendant in a case alleging infringement of U.S. Patent 6,820,204, relating to providing granular control over access to data. Result: all claims found invalid under §101. Affirmed by the Federal Circuit on Jan. 10, 2018. Contact: Andrew C. Mace, Esq., Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. (R)

220. *In re: The Matter of the 2016 Presidential Election,* 659 MD 2016 (Pa. Cmwlth. Ct., 2016). Served as an expert for intervenors opposing an action brought seeking a recount of votes in Pennsylvania on the grounds that the state's voting systems are unsecure and vulnerable to hacking by foreign actors. Petitioners discontinued the suit before hearing, refusing to post the required bond. Contact: Lawrence J. Tabas, Esq., Obermayer Rebmann Maxwell & Hippel LLP, One Penn Center, 19th Floor, 1617 John F. Kennedy Blvd., Philadelphia, PA 19103.

221. *Stein v. Cortés,* Case 2:16-cv-06287-PD (E.D. Pa.). Served as an expert for defendant Secretary of the Commonwealth of Pennsylvania in an action for a mandatory injunction to compel a recount and forensic examination of voting systems. Result: injunction denied. The Court's memorandum comments favorably on Dr. Shamos's qualification and testimony. Most claims have been dismissed on summary judgment. Case has settled. Contact: Timothy Gates, Esq., Chief Counsel, PA Department of State, 3306 North Office Bldg., Harrisburg, PA 17120. (R,T)

222. *Free Stream Media Corp. (d.b.a. Samba) v. Alphonso Inc.*, Case No. 3:17-cv-02107 (N.D. Cal., transferred from E.D. Tex.). Served as an expert for defendant Alphonso in an action alleging infringement of U.S. Patents 9,026,668 and 9,386,356, relating to a system for targeting data, such as advertising, to a device, such as a tablet, based on content that is identified as playing on a different device, such as a television. Alphonso won summary judgment of non-infringement. Contact: Neel Chatterjee, Esq., Goodwin Procter LLP, 601 Marshall Street, Redwood City, CA 94063. (D,R)

223. *Copart, Inc. v. Sparta Consulting, Inc.*, Case 2:14-cv-00046-KJM-CKD (E.D. Cal.). Served as an expert for defendant Sparta in an action alleging misappropriation of trade secrets relating to imaging batches of items to be offered at auction. Misappropriation counts were dropped during trial. Contact: Frederick Brown, Esq., Gibson, Dunn & Crutcher LLP, 555 Mission Street, Suite 3000, San Francisco, CA 94105. (D,R)

224. *Apple Inc. v. Masa LLC.*, IPR2016-00748, Patent Trial and Appeal Board (2016). Served as an expert for patent owner in an *inter partes* review of U.S. Patent 8,519,834, relating to a wearable device to alert a user to an incoming cellphone call. All challenged claims found invalid. Affirmed by the Federal Circuit. Contact: Robert M. Evans, Jr., Esq., Lewis Rice LLC, 600 Washington Avenue, Suite 2500, St. Louis, MO 63101. (R)

225. *Tele-Publishing, LLC v. Facebook, Inc. et al.,* Case 1:09-cv-11686-DPW (D. Mass.). Served as an expert for defendants in a case alleging infringement of U.S. Patent 6,253,216, relating to controlling access to information on personal web pages. Result: all claims found invalid under §101; judgment for defendants. Case settled during appeal to the Federal Circuit. Contact: Reuben Chen, Esq., Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. (R)

226. *Groupon, Inc. v. International Business Machines Corporation,* Case 1:16-cv-5064 (N.D. Ill.). Served as an expert for Groupon in a case alleging infringement of U.S. Patent 7,856,360, relating to gathering information from attendees at a venue. Case has settled. Contact: Saina Shamilov, Esq., Fenwick & West LLP, 801 California Street, Mountain View, CA 94041. (R)

227. *Stingray Digital Group Inc. v. Music Choice*, Patent Trial and Appeal Board. Served as an expert for petitioner in six *inter partes* reviews of U.S. Patents 7,320,025 (IPR2017-00888) and 9,351,045 (IPR2017-01191), relating to providing supplementing a broadcast media service with an on-demand, personalized media service and U.S. Patents 8,769,602 (IPR2017-01192), 9,357,245 (IPR2017-1193, IPR 2018-0114), relating to providing a visual complement to an audio program, and 9,414,121 (IPR 2017-1450), relating to systems and methods for providing on-demand entertainment. Trial has been instituted in '025, '045, '121 and '602. Patent owner requested adverse judgment in IPR2017-1193. Two claims survived in IPR2018-00114. Contact: Heath Briggs, Esq., Greenberg Traurig, LLP, 1200 17th St., Suite 2400, Denver, CO 80202. (D,R)

228. *Music Choice v. Stingray Digital Group Inc. et al.,* C.A. No. 2:16-CV-0586-JRG-RSP (E.D. Texas). Served as an expert for defendants in a case alleging infringement U.S. Patents 7,320,025 and 9,351,045, relating to providing supplementing a broadcast media service with an on-demand, personalized media service, U.S. Patents 8,769,602 and 9,357,245, relating to providing a visual complement to an audio program, and U.S. Patent 9,414,121, relating to systems and methods for providing on-demand entertainment. Case has settled. Contact: Joshua Raskin, Esq., Greenberg Traurig, LLP, MetLife Bldg., 200 Park Avenue, New York, NY 10166. (R)

229. *LivePerson, Inc. v. 24[7] Customer, Inc.*, IPR2017-00609, Patent Trial and Appeal Board. Served as an expert for patent owner in an *inter partes* review of U.S. Patent 6,970,553, relating to converting a voice call into a chat session. Four of six challenged claims were not found unpatentable. Contact: Bill Trac, Esq., O'Melveny & Myers LLP, Two Embarcadero Center, 28th Floor, San Francisco, CA 94111. (R)

230. *Blackberry Limited v. Blu Products, Inc.*, Case 1:16-cv-23535-FAM (S.D. Fla.). Served as an expert for defendants in a case alleging infringement of 15 patents, including U.S. Patent 6,271,605, relating to a battery disconnect system, U.S. Patent 8,169,449, relating to a multilayer graphics controller, and U.S. Patent 8,411,845, relating to the display of call logs on mobile phones. Case has settled. Contact: Victor Castellucci, Esq., Cozen O'Connor, 2 South Biscayne Blvd., 30th Floor, Miami, FL 33131. (R)

231. *Twitter, Inc. v. YouToo Technologies, LLC.*, Patent Trial and Appeal Board. Served as an expert for patent owner in two *inter partes* reviews of U.S. Patent 9,083,997 (IPR2017-00829,

IRP2017-00830), relating to publishing content on social media sites. All challenged claims found unpatentable. Contact: Samuel E. Joyner, Esq., Carrington, Coleman, Sloman & Blumenthal, LLP, 901 Main Street, Suite 5500, Dallas, TX 75202. (R)

232. *IPDEV Co. v. Ameranth, Inc.*, Case No. 3:14-cv-01303-GPC-JLB (S.D. Cal.). Served as an expert for defendant in an action to determine priority of invention among interfering patents involving U.S. Patents 6,384,850 and 6,871,325, assigned to Ameranth and relating to synchronous updating of restaurant menus on wireless devices, and U.S. Patents 5,991,739 and 8,738,449, relating to Internet ordering methods. Consolidated with Case 233, below. On summary judgment, the Court awarded priority to Ameranth. Contact: John W. Osborne, Esq., Osborne Law LLC, 33 Habitat Lane, Cortlandt Manor, NY 10567. (D,R)

233. *In re: Ameranth Patent Litigation*, Case No. 3:11-cv-01810-DMS-WSG (S.D. Cal.). Served as an expert for Ameranth in an action against numerous defendants alleging infringement of U.S. Patents 8,146,077, relating to synchronous updating of restaurant menus on wireless devices. All asserted claims were found invalid under 35 U.S.C. § 101, affirmed by the Federal Circuit. Contact: John W. Osborne, Esq., Osborne Law LLC, 33 Habitat Lane, Cortlandt Manor, NY 10567. (D,R)

234. *Google Inc. v. Spring Ventures, Ltd.*, IPR2017-01652 and 01653, Patent Trial and Appeal Board. Served as an expert for petitioner in *inter partes* reviews of U.S. Patent 8,661,094, relating to WWW addressing. Trial instituted in 2017-01653, denied in 2017-01652. Result: all claims of the '094 patent were determined to be unpatentable. Affirmed on appeal to the Federal Circuit. At oral argument, Dr. Shamos's qualifications were challenged unsuccessfully. Contact: Scott McKeown, Esq., Ropes & Gray, L.L.P., 2099 Pennsylvania Avenue, Washington, DC 20006-6807. (D,R)

235. *Rovi Guides, Inc. et al. v. Comcast Corporation et al.*, Case No. 1:16-cv-09278-JPO (S.D.N.Y.). Served as an expert for plaintiffs in an action alleging infringement of U.S. Patent 8,713,595, relating to electronic TV program guides and 9,172,987, relating to the use of markup language to alter the functionality of set-top boxes. Case has settled. Contact: Richard A. Kamprath, Esq., McKool Smith, 300 Crescent Court, Suite 1500, Dallas, TX 75201. (D,R)

236. *StrikeForce Technologies, Inc. v. Entrust, Inc. et al.*, Case No. 1:17-cv-00309-LMB-TCB (E.D. Va.). Served as an expert for plaintiff in an action alleging infringement of U.S. Patents 8,484,698, and 8,713,701, relating to out-of-band authentication using mobile devices. Case has settled. Contact: Josef Schenker, Esq., Ropes & Gray LLP, 1211 Avenue of the Americas, New York, NY 10036. (R)

237. *Level One Technologies, Inc. v. Penske Truck Leasing Co, Inc. and Penske Logistics, LLC*, Case No. 4:14-cv-1305-RWS (E.D. Mo.). Served as an expert for defendant in an action alleging trade secret misappropriation and contractual breach of confidentiality relating to a computer system for invoicing and rendering electronic payments in the trucking industry. Case has settled. Contact: Douglas Y. Christian, Esq., Ballard Spahr LLP, 1735 Market Street, 51st Floor, Philadelphia, PA 19103. (D,R)

238. *Uniloc USA Inc. et al. v. Netsuite Inc.*, Case No. 2:16-cv-00862-RWS (E.D. Texas) and *Uniloc USA Inc. et al. v. Nutanix Inc.*, Case No. 2:16-cv-01193-RWS (E.D. Texas). Served as an expert for plaintiff on claim construction issues in an action alleging infringement of U.S. Patent 6,324,578, relating to management of configurable application programs on a network. Later, the asserted claims were found invalid under 35 U.S.C. § 101. Contact: James J. Foster, Esq., Prince Lobel Tye LLP, One International Place, Suite 3700, Boston, MA 02110. (R)

239. *Muransky v. The Cheesecake Factory, Inc. et al.*, Case 2:17-cv-07569-CJC-RAO (C.D. Cal). Served as an expert for defendants in a case involving alleged violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681 ("FCRA") arising from display of more than five digits of a credit card number on customer receipts. Case has settled. Contact: John L. McManus, Esq., Greenberg Traurig, P.A., 401 E. Los Olas Blvd., Suite 2000, Fort Lauderdale, FL 33301. (R)

240. *Twilio, Inc. v. Telesign Corporation*, IPR2016-00451, Patent Trial and Appeal Board (2016). Served as an expert for petitioner in an *inter partes* review of U.S. Patent 8,687,038, relating to verifying an online registration via an out-of-band telephone connection. Trial was not instituted. Contact: Contact: Carrie J. Richie, Esq., Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. (R)

241. *Twilio, Inc. v. Telesign Corporation*, IPR2016-01688, Patent Trial and Appeal Board (2016). Served as an expert for petitioner in an *inter partes* review of U.S. Patent 9,300,792, relating to verification of telephone users based on characteristics of the telephone number, such as carrier and geographic location. All challenged claims found unpatentable. Contact: Contact: Carrie J. Richie, Esq., Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. (R)

242. *EdiSync Systems, LLC v. Adobe Systems, Inc.*, Civil Action 12-cv-02231-MSK-MEH (D. Colo.). Served as an expert for Defendant Adobe in a case alleging infringement of U.S. Patent 5,799,320, relating to multi-author document editing systems. Case has settled. Contact: David Sipiora, Esq., Kirkpatrick Townsend & Stockton LLP, Suite 600, 1400 Wewatta Street, Denver, CO 80202.

243. *Ford Motor Company v. Versata Software, Inc. et al.*, Case No. 2:15-cv-10628-MFL-EAS (E.D. Mich.). Served as an expert for defendant/counter-plaintiff Versata in a declaratory judgment action relating to alleged infringement of U.S. Patents 5,825,651, 6,405,308 and 6,675,294, relating to product configuration through a graphical user interface; U.S. Patent 7,882,057, relating to complex product configuration using submodels; U.S. Patents 7,200,582 and 7,464,064, relating to checking the consistency of a product configuration model using set equations; and U.S. Patent 8,805,825, relating to product configuration in which attributes are prioritized. Result: jury vedict for Versata for $105 million. Contact: Steve Mitby, Esq., Mitby Pacholder Johnson PLLC, 1001 McKinney St., Suite 925, Houston, TX 77002. (D,R)

244. *Improved Search LLC v. Microsoft Corporation*, C.A. No. 16-cv-650-JFB-SRF (D.Del.). Served as an expert for plaintiff in an action alleging infringement of U.S. Patents 6,604,101 and 7,516,154, relating to methods and systems for translingual searching. Plaintiff sought a judgment of non-infringement so claim constructions could be appealed to the Federal Circuit.

Result: affirmed. Contact: Robert Yorio, Esq., Carr & Ferrell LLP, 120 Constitution Drive, Menlo Park, CA 94025. (D,R)

245. *Comcast Cable Communications, LLC v. Rovi Guides, Inc.*, IPR2017-00866, IPR2017-00867, Patent Trial and Appeal Board. Served as an expert for patent owner in *inter partes* reviews of U.S. Patent 8,713,595, relating to electronic television program guides. All challenged claims found unpatentable. Contact: Josef B. Schenker, Ropes & Gray LLP, 1211 Avenue of the Americas, New York, NY 10036. (D,R)

246. *Comcast Cable Communications, LLC v. Rovi Guides, Inc.*, IPR2017-00950, IPR2017-00951, IPR2017-00952, Patent Trial and Appeal Board. Served as an expert for patent owner in *inter partes* reviews of U.S. Patent 8,006,263, relating to electronic television program guides. All challenged claims found unpatentable. Contact: Josef B. Schenker, Ropes & Gray LLP, 1211 Avenue of the Americas, New York, NY 10036. (D,R)

247. *Unified Patents, Inc. v. Anuwave LLC.*, IPR2018-00223, Patent Trial and Appeal Board. Served as an expert for petitioner in *inter partes* reviews of U.S. Patent 8,295,862, relating to enabling short message system (SMS) communication without using IP services. Terminated by settlement. Contact: Robert High, Esq., Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, 271 17th St. N.W., Suite 1400, Atlanta, GA 30363-6209. (R)

248. *Comcast Cable Communications, LLC v. Rovi Guides, Inc.*, IPR2017-01048, IPR2017-01049, IPR2017-01050, Patent Trial and Appeal Board. Served as an expert for patent owner in *inter partes* reviews of U.S. Patent 8,578,413, relating to electronic television program guides. All challenged claims found unpatentable. Contact: Josef B. Schenker, Ropes & Gray LLP, 1211 Avenue of the Americas, New York, NY 10036. (D,R)

249. *Comcast Cable Communications, LLC v. Rovi Guides, Inc.*, IPR2017-01065, IPR2017-01066, IPR2017-01143, Patent Trial and Appeal Board. Served as an expert for patent owner in *inter partes* review of U.S. Patent 8,046,801, relating to electronic television program guides. All challenged claims found unpatentable. Contact: Josef B. Schenker, Ropes & Gray LLP, 1211 Avenue of the Americas, New York, NY 10036. (D,R)

250. *DevFactory FZ-LLC v. Magnitude Software, Inc.*, Arbitration WIPOA300617. Served as an expert for Claimant DevFactory in an arbitration relating to a claim of breach of a software Technology Services Agreement. Arbitration has terminated. Contact: Steve Mitby, Esq., Ahmad, Zavitsanos, Anaipakos, Alavi & Mensing P.C., 1221 McKinney, Suite 2500, Houston, TX 77010.

251. *BookIT Oy Ajanvarauspalvelu v. Bank of America Corporation et al.*, 3:17-cv-02577-K (N.D. Texas). Served as an expert for BookIT in an action alleging infringement of U.S. Patents 8,589,194 and 9,177,268, relating to mediating communications between a service provider and a user in a telecommunications network. Plaintiff sought a judgment of non-infringement so that claim constructions could be appealed to the Federal Circuit, which affirmed. Contact:

Richard A. Kamprath, Esq., McKool Smith, 300 Crescent Court, Suite 1500, Dallas, TX 75201. (D,R)

252. *Promptu Systems Corporation v. Comcast Corporation et al.*, 2:16-cv-06516-JS (E.D. Pa.). Served as an expert for plaintiff in an action alleging infringement of U.S. Patents 7,047,196, 7,260,538 and RE44,326, relating to voice control of television set-top boxes. Plaintiff is appealing an adverse claim construction. Contact: Robert Yorio, Esq., Carr & Ferrell LLP, 120 Constitution Drive, Menlo Park, CA 94025. (D,R)

253. *Snap Inc. v. Vaporstream, Inc.*, IPR2018-00200, IPR2018-00312, IPR2018-00369, IPR2018-00397, IPR2018-00404, IPR2018-00408, IPR2018-00416, IPR2018-00439, IPR2018-00455, IPR2018-00458, Patent Trial and Appeal Board. Served as an expert for patent owner in *inter partes* reviews of U.S. Patents 8,886,739, 8,935,351, 9,306,885, 9,306,886, 9,313,155, 9,313,156, 9,313,157, 9,338,111 and 9,413,711, relating to reducing traceability of electronic messages. In IPR2018-00312, IPR2018-00369, IPR2018-00404 and IPR2018-00408 and IPR2018-00458, all challenged claims were found unpatentable. In IPR2018-00397, IPR2018-00416, IPR2018-00439 and IPR2018-00455, and IPR2018-00458, all challenged claims were found patentable. Contact: Douglas R. Wilson, Esq., Heim, Payne & Chorush, LLP, Heritage Plaza, 111 Bagby, Suite 2100, Houston, TX 77002. (R)

254. *Shopify, Inc. v. DDR Holdings, LLC*, IPR2018-01008, IPR2018-01009, IPR2018-01010, IPR2018-01011, IPR2018-01012, IPR2018-01014, Patent Trial and Appeal Board. Served as an expert for petitioner in *inter partes* reviews of U.S. Patents 8,515,825, 9,043,228, and 9,639,876, relating to online affiliate marketing. In 2018-01008 and 2018-01009, the PTAB found all challenged claims patentable. In 2018-01010, 2018-01011, 2018-01012 and 2018-01014, the PTAB found most challenged claims unpatentable, affirmed by the Federal Circuit in 2018-01011, 2018-01012 and 2018-01014. Contact: Jinnie L. Reed, Esq., Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C., One Financial Center, Boston. MA 02111. (D,R)

255. *Election Systems & Software, LLC v. Dominion Voting Systems, Inc.*, 1:17-cv-01172-CJB (D. Del.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patent 8,991,701, relating to an accessible voting system. Case has settled. Contact: Robert M. Evans, Jr., Esq., Lewis Rice LLC, 600 Washington Avenue, Suite 2500, St. Louis, MO 63101.

256. *General Motors LLC et al. v. Dorman Products, Inc. et al.*, 2:15-cv-129170-VAR-EAS (E.D. Mich.). Served as an expert for plaintiff in a case alleging copyright infringement and violation of the anti-circumvention provisions of the Digital Millennium Copyright Act relating to offloading of transmission control software from automobiles. Case has settled. Contact: Aaron A. Barlow, Esq., Jenner & Block LLP, 353 North Clark Street, Chicago, IL 60654-3456.

257. *PPS Data, LLC v. Jack Henry & Associates, Inc.,* Case 2:18-cv-00007-JRG (E.D. Texas). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 7,181,430, 7,216,106, 7,440,924, 7,624,071 and 8,126,809, relating to methods for processing check images in electronic payment systems. The '430, '924, '071 and '809 patent were found invalid by the Court under 35 U.S.C. § 101. After a jury trial, all asserted claims of the '106

patent were found not infringed and invalid. Contact: Anthony H. Son, Esq., Maddox Edwards, PLLC, 1900 K Street NW, Suite 725, Washington, DC 20006. (D,R,T)

258. *NEXT Payment Solutions, Inc. v. CLEAResult Consulting, Inc.,* Case 1:17-cv-08829 (N.D. Illinois). Served as an expert for defendant in a case alleging misappropriation of trade secrets relating to a system for managing energy rebate appointments and inspections. The trade secret counts were dismissed on summary judgment. Contact: Anthony Fuga, Esq., Holland & Knight LLP, 131 S. Dearborn Street, 30th Floor, Chicago, IL 60603. (R)

259. *Certain Digital Video Receivers and Related Hardware and Software Components*, USITC Inv. No. 337-TA-1103. Served as an expert for Complainants Rovi Corporation et al. against Comcast Corporation et al. in an International Trade Commission proceeding involving alleged infringement of U.S. Patents 9,294,799, relating to resumption on a second device of video paused on a first device, and 9,578,363, relating to providing video in a format suitable for a particular device. Those patents were subsequently dropped. Dr. Shamos testified about his observation of user focus groups. The ITC issued an exclusion order, upheld by the Federal Circuit. Contact: Richard A. Kampraith, Esq., McKool Smith, 300 Crescent Court, Suite 1500, Dallas, TX 75201. (D,R,T)

260. *ARM Ltd. et al. v. Complex Memory, LLC*, IPR2019-00053, IPR2019-00058, Patent Trial and Appeal Board. Served as an expert for petitioners in *inter partes* reviews of U.S. Patent 5,890,195, relating to cache memory (SRAM) integrated with main memory (DRAM) and U.S. Patent 6,658,576, relating to an energy-conserving computer operating system. Outcome: both IPRs terminated by settlement. Contact: Kevin Anderson, Esq., Duane Morris LLP, 505 9th Street, NW, Suite 1000, Washington, DC 20004-2166. (R)

261. *Supercell Oy v. Gree, Inc.*, PGR2018-00070, PGR2018-00071, Patent Trial and Appeal Board. Served as an expert for patent owner in post-grant reviews of U.S. Patents 9,770,656 and 9,770,664, relating to user interfaces for multiplayer online games. Institution denied in both PGRs. Contact: Scott McKeown, Esq., Ropes & Gray, L.L.P., 2099 Pennsylvania Avenue, Washington, DC 20006-6807. (R)

262. *Amazon Services, LLC v. South Carolina Dept. of Revenue*, Docket No. 17-ALJ-0238-CC. (S.C. Admin. Ct.). Served as an expert for South Carolina in a tax dispute relating to online sales through Amazon's Merchant Fulfillment Network. Result: Amazon found liable to pay tax. Contact: John Hoefer, Esq., Willoughby & Hoefer, P.A., 940 Richland St., P.O. Box 8416, Columbia, SC 29202-8416. (D)

263. *Supercell Oy v. Gree, Inc.*, PGR2019-00018, Patent Trial and Appeal Board. Served as an expert for patent owner in a post-grant review of U.S. Patent 9,891,799, relating to a method for moving a plurality of objects in a computer game. All claims found unpatentable under 35 U.S.C. § 101. Affirmed by the Federal Circuit. Contact: Scott McKeown, Esq., Ropes & Gray, L.L.P., 2099 Pennsylvania Avenue, Washington, DC 20006-6807. (D,R)

264. *Beal v. Outfield Brew House, LLC.,* Case 2:18-cv-4028 (W.D. Missouri). Served as an expert for plaintiff, representative of a putative class, in a case alleging violation of the

Telephone Consumer Protection Act, 47 U.S.C. § 227, specifically on the issue whether certain dialing systems constitute an "Automatic Telephone Dialing System" under the statute. The District Court ruled for defendant on summary judgment based on statutory interpretation, now on appeal to the Eighth Circuit. Contact: Bill Kenney, Esq., Bill Kenney Law Firm, LLC., 1100 Main St. Suite 1800, Kansas City, MO 64105. (D,R)

265. *Smartmatic USA Corporation v. Election Systems & Software, LLC,* IPR2019-00531, Patent Trial and Appeal Board. Served as an expert for patent owner in an inter partes review of U.S. Patent 8,096,471, relating to a ballot marking device having an attached ballot box and IPR2019-00527 of U.S. Patent 7,753,273. All '471 claims found patentable. Four '273 claims found patentable. Contact: Robert M. Evans, Jr., Esq., Lewis Rice LLC, 600 Washington Avenue, Suite 2500, St. Louis, MO 63101. (D,R)

266. *Curling et al. v. Raffensperger et al.,* Case 1:17-CV-2989AT (N.D. Georgia). Served as an expert for defendants Secretary of State and State Election Board in a case in which plaintiffs seek an injunction of forbid use of DRE voting machines in Georgia in 2019. Preliminary injunction denied as to the November 2019 election. Contact: Vincent Russo, Esq., Robbins Ross Alloy Belinfante Littlefield LLC, 500 14th Street N.W., Atlanta, GA 30318. (D,R)

267. *Smith v. Truman Road Development, LLC d/b/a No OtherPub,* Case 4:18-cv-670-NKL (W.D. Missouri). Served as an expert for plaintiff, representative of a putative class, in a case alleging violation of the Telephone Consumer Protection Act, 47 U.S.C. § 227, specifically on the issue whether certain dialing systems constitute an "Automatic Telephone Dialing System" under the statute. The District Court ruled for defendant on summary judgment based on statutory interpretation. Contact: Bill Kenney, Esq., Bill Kenney Law Firm, LLC., 1100 Main St. Suite 1800, Kansas City, MO 64105. (R)

268. *J. T. Hand et al. v. Beach Entertainment, LLC d/b/a Shark Bar,* Case 4:18-cv-668-NKL (W.D. Missouri). Served as an expert for plaintiff, representative of a putative class, in a case alleging violation of the Telephone Consumer Protection Act, 47 U.S.C. § 227, specifically on the issue whether certain dialing systems constitute an "Automatic Telephone Dialing System" under the statute. Partial summary judgment was granted, now on appeal to the Eighth Circuit. Contact: Bill Kenney, Esq., Bill Kenney Law Firm, LLC., 1100 Main St. Suite 1800, Kansas City, MO 64105. (R)

269. *WhereverTV, Inc. v. Comcast Corporation, et al.,* Case 2:18-cv-00529-UA-CM (M.D. Florida). Served as an expert for plaintiff in a case alleging infringement of U.S. Patent 8,656,431, relating to a system for integrating television and IPTV channels into a global interactive program guide. Contact: Adam Sanderson, Esq., Reese Marketos LLP, 750 N. St. Paul St., Suite 600, Dallas, TX 75201. (R)

270. *Droplets, Inc. v. Nordstrom, Inc.*, Case 3:12-CV-04049-JST (N.D. Cal.). Served as an expert for defendant in an action alleging infringement of U.S. Patent 8,402,115, relating to delivering interactive links for presenting applications on a client computer. Case has settled.

Contact: Benjamin Kleinman, Esq., Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center Suite 1900, San Francisco, CA 94111. (D,R)

271. *Droplets, Inc. v. Yahoo!, Inc.*, Case 3:12-CV-03733-JST (N.D. Cal.). Served as an expert for defendant in an action alleging infringement of U.S. Patent 8,402,115, relating to delivering interactive links for presenting applications on a client computer. At trial, Plaintiff sought $250 million, was awarded $15 million. Contact: Kevin P. Anderson. Esq., Duane Morris LLP, 505 9th Street, N.W., Suite 1000, Washington, DC 20004-2166. (D,R,T)

272. *Square, Inc. v. 4361423 Canada, Inc. d/b/a AnywhereCommerce*, IPR2019-01651, IPR2019-01652, IPR2019-01653, and IPR2019-001654, Patent Trial and Appeal Board. Served as an expert for petitioner in inter-partes reviews of U.S. Patents 9,443,239, 9,613,351, and 9,818,107, relating to an attachment to a cellphone to facilitate credit card transactions. Result: all challenged claims umpatentable in all four IPRs. Contact: David Tennant, Esq., White & Case, L.L.P., 701 Thirteenth Street, NW, Washington, DC 20005. (R)

273. *Uniloc 2017 LLC. v. Netflix, Inc. et al.*, Lead Consolidated Case SACV8:18-cv-2055-GW-DFMx (C.D. Cal.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 8,497,609, relating to tracking the amount of time a presentation is watched online, and 9,721,273, relating to aggregating and presenting audio and video over a network. Case has settled. Contact: Sal Lim, Esq., Feinberg Day Kramer Alberti Lim Tonkovich & Belloli LLP, 1600 El Camino Real, Suite 280, Menlo Park, CA 94025. (R)

274. Comcast Cable Communications, LLC v. WhereverTV, Inc., IPR2019-01482, and IPR2019-001483, Patent Trial and Appeal Board. Served as an expert for Patent Owner in inter-partes reviews of U.S. Patent 8,656,431, relating to a system for integrating television and IPTV channels into a global interactive program guide. Institution denied in both cases. Contact: Adam Sanderson, Esq., Reese Marketos LLP, 750 N. St. Paul St., Suite 600, Dallas, TX 75201. (R)

275. Boom! Payments, Inc. v. Stripe, Inc. et al., Case 3:19-cv-0050-VC (N.D. Cal.). Served as an expert for Defendants Shopify, Inc. and Shopify (USA) Inc. in an action alleging infringement of U.S. Patents 8,429,084, and 9,235,857, relating to a system for confirming that a physical exchange of goods has occurred in an online transaction. All asserted claims found invalid under 35 U.S.C. § 101 upon Defendants' motion to dismiss. Contact: Vincent M. Ferraro, Esq., Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C., Chrysler Center, 666 Third Avenue, New York, NY 10017.

276. Curb Mobility, LLC. v. Kaptyn, Inc. et al., Case 2:18-cv-02416-MMD-GWF (D. Nev.). Served as an expert for Defendants in an action alleging infringement of U.S. Patent 6,347,739, relating to a system for accepting credit cards in taxicabs. All asserted claims found invalid under 35 U.S.C. § 101. Contact: Robert Yorio, Esq., Carr & Ferrell LLP, 120 Constitution Drive, Menlo Park, CA 94025. (R)

277. Canon, Inc. v. TCL Electronics Holdings, Ltd., et al., Case 2:18-cv-00546-JRG (E.D. Texas). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patent

7,810,130, relating to buffering video content, U.S. Patent 7,746,413, relating to interpreting instructions from a television remote control, and U.S. Patents 8,078,767, 8,346,986 and 8,713,206, relating to controlling a digital display when an external device has been disconnected. Case has settled. Contact: Kyotaro Ozawa, Esq., Paul Hastings LLC, Ark Hills Sengokuyama Mori Tower, Fortieth Floor 1-9-10 Roppongi, Minato-ku, Tokyo 106-0032 Japan. (D,R)

278. *Uniloc 2017 LLC v. Paychex, Inc.*, Case No. 1:19-cv-11272-RGS (D. Mass.), consolidated for certain purposes with *Uniloc 2017 LLC v. AthenaHealth Inc.*, Case No. 1:19-cv-11278-RGS (D. Mass.). Served as an expert for plaintiff in actions alleging infringement of U.S. Patent 6,324,578, relating to management of configurable application programs on a network. Paychex case dismissed for lack of jurisdiction. Cases have settled. Contact: James J. Foster, Esq., Prince Lobel Tye LLP, One International Place, Suite 3700, Boston, MA 02110. (D,R)

279. *H2O Resources, LLC v. Oilfield Tracking Services, LLC*, AAA Case No. 01-18-0003 6309 (Houston, Texas). Served as an expert for defendants in an arbitration alleging misappropriation of trade secrets under 18 U.S.C. § 1836 and 12 P.S. § 5301 (Pennsylvania) relating to a system for tracking movement of produced water generated from oil and gas drilling. Matter has settled. Contact: Paul Greco, Esq., Fisher Philips LLP, 150 N. Radnor Chester Road, Suite C300, Radnor, PA 19087. (D,R)

280. *J.T. Hand et al. v. ARB KC, LLC d/b/a Angels Rocks Bar,* Case 4:19-cv-108-BCW (W.D. Missouri). Served as an expert for plaintiff, representative of a putative class, in a case alleging violation of the Telephone Consumer Protection Act, 47 U.S.C. § 227, specifically on the issue whether certain dialing systems constitute an "Automatic Telephone Dialing System" under the statute. Contact: Bill Kenney, Esq., Bill Kenney Law Firm, LLC., 1100 Main St. Suite 1800, Kansas City, MO 64105. (R)

281. *Doohan et al. v. CTB Investors, LLC d/b/a PBR Big Sky Cowboy Bar et al.,* Case 4:19-cv-111-FJG (W.D. Missouri). Served as an expert for plaintiff, representative of a putative class, in a case alleging violation of the Telephone Consumer Protection Act, 47 U.S.C. § 227, specifically on the issue whether certain dialing systems constitute an "Automatic Telephone Dialing System" under the statute. Contact: Bill Kenney, Esq., Bill Kenney Law Firm, LLC., 1100 Main St. Suite 1800, Kansas City, MO 64105. (R)

282. *Taylor et al. v. KC Vin, LLC d/b/a/ Pizza Bar, et al.,* Case 4:19-cv-110-NKL (W.D. Missouri). Served as an expert for plaintiff, representative of a putative class, in a case alleging violation of the Telephone Consumer Protection Act, 47 U.S.C. § 227, specifically on the issue whether certain dialing systems constitute an "Automatic Telephone Dialing System" under the statute. Contact: Bill Kenney, Esq., Bill Kenney Law Firm, LLC., 1100 Main St. Suite 1800, Kansas City, MO 64105. (R)

283. *The Thomas L. Pearson and The Pearson Family Members Foundation, et al. v. The University of Chicago,* Case 4:18-cv-00099-GKF-FHM (N.D. Oklahoma). Serving as an expert for plaintiffs in an action alleging breach of an agreement granting $100 million to the

University of Chicago. Contact: Isaac Ellis, Esq., Conner & Winters, LLP, 4000 One Williams Center, Tulsa, OK 74172-0148. (D,R)

284. *ESW Holdings, Inc. v. Roku, Inc.,* Case 6:19-cv-00044-ADA (W.D. Texas). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patent 9,420,349, relating to monitoring a digital media stream and identifying media objects through fingerprinting. Jury verdict for defendent. Contact: Conor Civins, Esq., Bracewell LLP, 111 Congress Avenue, Suite 2300, Austin, TX 78701-4061 (D,R,T)

285. *Apple, Inc. v. Fintiv, Inc.,* IPR2020-00019, Patent Trial and Appeal Board. Served as an expert for Patent Owner in an inter-partes review of U.S. Patent 8,843,125, relating to a system and method for managing a mobile wallet through a Trusted Service Manager (TSM). Institution denied. Contact: Marcus Barber, Esq., Kasowitz Benson Torres LLP, 333 Twin Dolphin Drive, Suite 200, Redwood Shores, CA 94065. (D, R)

286. *Election Systems & Software, LLC v. Hart InterCivic, Inc.,* PGR2020-00031, Patent Trial and Appeal Board. Served as an expert for petitioner in a post-grant review of U.S. Patent 10,445,966, relating to conversion of printed ballots into cast vote records by optical character recognition. Result: all challenged claims unpatentable. Federal Circuit appeal was dismissed by Patent Owner. Contact: Robert M. Evans, Jr., Esq., Lewis Rice LLC, 600 Washington Avenue, Suite 2500, St. Louis, MO 63101. (D,R)

287. *Launius v. Flores, in her official capacity as Presiding Officer, Chair of Trustees, of Dallas County Community College District*, Cause DC-19-08429 (Dist. Ct., Dallas Cty., Texas). Served as an expert for contestee in an action alleging that an election held May 4, 2019 approving a $1 billion bond issue should be overturned because "the true outcome of the election cannot be ascertained." After a bench trial, the Court granted judgment in favor of contestee. Affirdmed by the Court of Appeals. The Texas Supreme Court declined review. Contact: Adam Rothey, Esq., Thompson & Horton LLP, 500 N. Akard St., Suite 3150, Dallas, TX 75201. (D,T)

288. *Slyce Acquisition, Inc. v. Syte - Visual Conception Ltd. et al.,* Case 6:19-cv-00257-ADA (W.D. Texas). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patent 9,152,624, relating to navigating Web content via image analysis. Case has settled. Contact: Michael Chibib, Esq., Bracewell LLP, 111 Congress Avenue, Suite 2300, Austin, TX 78701-4061 (R)

289. *Early Warning Services, LLC v. William Grecia,* IPR2020-00763, Patent Trial and Appeal Board. Served as an expert for petitioner in an inter partes review of U.S. Patent 8,887,308, relating to generation of tokens authenticating users seeking access to digital cloud content. Review was not instituted, but the patent was found invalid on § 101 grounds in litigation. Contact: Cory Smith, Esq., Bryan Cave Leighton Paisner LLP, Two North Central Avenue, Suite 2100, Phoenix, AZ 85004-4406. (R)

290. *Supercell Oy v. Gree, Inc.*, PGR2020-00063, Patent Trial and Appeal Board. Served as an expert for patent owner in a post-grant review of U.S. Patent 10,406,432, relating to a method for providing information in a head-mounted display based on gaze sensing. Institution

denied. Contact: Scott McKeown, Esq., Ropes & Gray, L.L.P., 2099 Pennsylvania Avenue, Washington, DC 20006-6807. (R)

291. *Digital Retail Apps, Inc. v. H-E-B Grocery Company, LP,* Case 6:19-cv-00167-ADA (W.D. Texas). Served as an expert for defendant in an action alleging infringement of U.S. Patents 9,262,781, and 9,934,506, relating to use of QR codes in point-of-sale electronic payment applications. Case settled before trial. Contact: Andrew Klein, Esq., Perkins Coie LLP, 3150 Porter Drive, Palo Alto, CA 94304-1212. (D,R)

292. *HLFIP Holding, Inc. d/b/a/ Smart Communications IP Holdings v. Rutherford County, Tennessee et al.,* Case 3:19-cv-00714 (M.D. Tenn.). Served as an expert for intervenor VendEngine, Inc. in an action alleging infringement of U.S. Patent 10,291,167, relating to a computerized method of eliminating contraband in mail directed to correctional facilities. Defendant and intervenor prevailed on judgment on the pleadings that the patent was ineligible under 35 U.S.C. § 101. Contact: W. Edward Ramage, Esq., Baker Donelson, Bearman, Caldwell & Berkowitz, P.C., Monarch Plaza, Suite 1600, 3414 Peachtree Road N.E., Atlanta, GA 30326. (D,R)

294. *Broadband iTV, Inc. v. DISH Network, L.L.C.*, Case 6:19-cv-716-ADA (W.D. Texas). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patents 9,648,388, 9,998,791, 10,023,026 and 10,506,269, relating to hierarchical navigation of video-on-demand television menus. Case has settled. Contact: Sal Lim, Esq., Kramer Day Alberti Lim Tonkovich & Belloli LLP, 577 Airport Boulevard, Suite 250, Burlingame, California 94010. (D,R)

295. *Arendi S.A.R.L. v. Blackberry Limited et al.*, Case 1:12-cv-01595-LPS (D. Del.). Serving as an expert for Defendant in an action alleging infringement of U.S. Patents 7,917,843 and 8,306,993, relating to a touchscreen mechanism for providing name and address handling by an associated information system. Contact: Jason W. Cook, Esq., McGuireWoods LLP, 2000 McKinney Ave., Suite 1400, Dallas, TX 75201. (D,R)

296. *Unified Patents, LLC v. Monarch Networking Solutions LLC,* IPR2020-01708, Patent Trial and Appeal Board. Served as an expert for petitioner in an inter partes review of U.S. Patent 7,756,507, relating to out-of-band authentication to obtain access to a digital network. All challenged claims found unpatentable. Contact: John M. Baird, Esq., Duane Morris LLP, 505 9th Street, N.W., Suite 1000, Washington, DC 20004-2166. (R)

297. *Aqua Connect, Inc. et al. v. TeamViewer U.S. Inc. et al.*, Case 1:18-cv-01572-MN (D. Del.). Served as an expert for Plaintiffs in an action alleging infringement of U.S. Patents RE46,386 and 8,924,502, relating to updating a user session in a Mach-derived system environment. At trial, the jury awarded Plaintiffs $5.7 million, before prejudgment interest. Contact: Ryan E. Hatch, Esq., Hatch Law, P.C., 13323 Washington Blvd., Suite 100, Los Angeles, CA 90066. (D,R,T)

298. *PayPal, Inc. v. RetailMeNot, Inc.,* Case 6:20-cv-00339-ADA (W.D. Texas). Served as an expert for PayPal in an action alleging infringement by RetailMeNot of U.S. Patents 6,917,961 and 7,693,937, relating to evolving interactive browser dialog boxes, U.S. Patent 7,659,905,

relating to pre-fetching data on a network, U.S. Patents 8,909,248 and 9,654,932, relating to provision of location-based services, and U.S. Patents 9,053,514 and 9,082,153, relating to automatic rebate and coupon redemption, and alleging in counterclaims infringement by PayPal of U.S. Patents 10,296,931, and 10,489,814, relating to accessing promotional offers displayed on websites by circumventing secure sandbox protections. Case has settled. Contact: Steve Marshall, Esq., Fish & Richardson, P.C., 1000 Maine Avenue, S.W., Suite 1000, Washington, DC 20024.

299. *Rovi Guides, Inc. et al. v. Comcast Corporation et al.*, Case No. 2:18-cv-00253-AG-FFM (C.D. Cal.). Served as an expert for plaintiffs in an action alleging infringement of U.S. Patents 7,827,585, relating to electronic TV program guides, 9,294,799, relating to an on-demand media delivery system, 9,369,741, relating to an interactive television reminder system, 9,578,363, relating to accessing video content via standard and high-definition channels, 9,621,956, relating to a television transport control interface, and 9,668,014, relating to methods for storing video assets. Case has settled. Contact: Richard A. Kamprath, Esq., McKool Smith, 300 Crescent Court, Suite 1500, Dallas, TX 75201.

300. *RetailMeNot, Inc. v. Honey Science, LLC,* Case 1:18-cv-00937-CFC-MPT (D. Del.). Served as an expert for defendant in an action alleging infringement of U.S. Patents 9,626,688, 10,290,015, 10,296,931, and 10,489,814, relating to accessing promotional offers displayed on websites by circumventing secure sandbox protections. Case has settled. Contact: Richard Birnholz, Esq., Irell & Manella LLP, 1800 Avenue of the Stars, Suite 900, Los Angeles, CA 90067-4276.

301. *Certain Video Processing Devices, Components Thereof, and Digital Smart Televisions Containing the Same*, USITC Inv. No. 337-TA-1222. Served as an expert for Complainant DivX, LLC against numerous smart television manufacturers in an International Trade Commission proceeding involving alleged infringement of, *inter alia*, U.S. Patent 8,832,297, relating to multiphase adaptive bitrate streaming. Case has settled. Contact: Jessica Perry, Esq., Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C., One Financial Center, Boston, MA 02111.

302. *Google LLC v. Sonos, Inc.*, Case No. 3:20-cv-03845-EMC (N.D. Cal.). Serving as an expert for Google in an action alleging infringement of U.S. Patent 7,065,206, relating to echo and noise control, 7,899,187, relating to digital rights management, 8,583,489, relating to notification of availability of media content, 10,140,375, relating to personalized network searching, and 10,229,586, relating to communication via wireless sensor systems. Contact: Patrick D. Curran Esq., Quinn Emanuel Urquhart & Sullivan LLP, 111 Huntington Avenue, Suite 520, Boston, MA 02199. (R)

303. *Hitel Technologies LLC v. Nike, Inc.,* Case 6:20-cv-00591-ADA (W.D. Texas). Served as an expert for Nike in an action alleging infringement of U.S. Patent 7,689,617, relating to adaptive learning during Web navigation. Case was dropped by plaintiff during claim construction. Contact: Christopher Renk, Esq., Arnold & Porter Kaye Scholer LLP, 70 West Madison Street, Suite 4200, Chicago, IL 60602-4231.

304. *Hitel Technologies LLC v. Levi Strauss & Co.*, Case 6:20-cv-00589-ADA (W.D. Texas). Served as an expert for Levi Strauss in an action alleging infringement of U.S. Patent 7,689,617, relating to adaptive learning during Web navigation. Case was dropped by plaintiff during claim construction. Contact: Robert A. McFarlane, Esq., Hanson Bridgett LLP, 425 Market Street, 26th Floor, San Francisco, CA 94105.

305. *Unified Patents, LLC v. Caselas, LLC,* IPR2021-00799, Patent Trial and Appeal Board. Served as an expert for petitioner in an inter partes review of U.S. Patent 9,716,691, relating to providing information about charge-backs in credit reports. Result: all challenged claims found unpatentable. See Final Written Decision. Contact: Larissa Bifano, Esq., DLA Piper LLP, 33 Arch Street, 26th Floor, Boston, MA 02110-1447. (D,R)

306. *Fortinet, Inc. v. Forescout Technologies, Inc.*, Case 3:20-cv-03343-EMC-ADA (N.D. Cal.). Serving as an expert for plaintiff in an action alleging infringement of U.S. Patents 8,458,314, relating to administration of network security privileges, 9,369,299, relating to methods for controlling remote network access, 9,503,421, relating to security information and event management, 9,894,034, relating to configuration of network endpoint security, and 9,948,662, relating to application layer network security. Contact: Rachel Blitzer, Esq., Skadden, Arps, Slate, Meagher & Flom LLP, One Manhattan West, New York, NY 10001. (R)

307. *Delaware North iGaming, Inc. v. Miomni Gaming Ltd. et al.,* C.A. 2019-0301-JTL (Del. Ch.). Served as a court-appointed expert in a matter alleging breach of contract to provide software and computing services. Case has settled. Contact: Vice-Chancellor J. Travis Laster, Court of Chancery, 500 North King Street, Wilmington, DE 19801.

308. *Zillow Group et al. v. International Business Machines Corp.*, IPR2020-01656, Patent Trial and Appeal Board. Served as an expert for patent owner in an *inter partes* review of U.S. Patent 8,315,904, relating to a computerized method for managing promotions. Review was instituted, but all Challenged Claims were found patentable. Contact: Gautam Patnaik, Esq., Desmarais, LLP, 1701 Pennsylvania Avenue NW, Suite 200, Washington, D.C. 20006. (D,R)

309. *ByteDance Ltd. and TikTok Inc. v. Triller, Inc.*, IPR2021-00099, Patent Trial and Appeal Board. Served as an expert for patent owner in an *inter partes* review of U.S. Patent 9,691,429, relating to systems and methods for creating music videos synchronized with an audio track. Case has settled. Contact: Brent Lorimer, Esq., Workman Nydegger, 60 East South Temple, Suite 1000, Salt Lake City, UT 84111. (D,R)

310. *Broadband iTV, Inc. v. Amazon.Com, Inc. et al.*, Case 6:20-cv-921-ADA (W.D. Texas). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patents 9,648,388, 9,973,826, 10,023,026, 10,506,269, 10,536,750 and 10,536,751, relating to hierarchical navigation of video-on-demand television menus. Asserted claims found invalid as non-statutory. Now on appeal to the Federal Circuit. Contact: Sal Lim, Esq., Kramer Day Alberti Lim Tonkovich & Belloli LLP, 577 Airport Boulevard, Suite 250, Burlingame, California 94010. (D,R)

311. *DISH Network, L.L.C, v. Broadband iTV, Inc.,* IPR2020-01267, Patent Trial and Appeal Board. Served as an expert for patent owner in in an *inter partes* review of U.S. Patent

10,023,026, relating to hierarchical navigation of video-on-demand television menus. Case has settled. Contact: Sal Lim, Esq., Kramer Day Alberti Lim Tonkovich & Belloli LLP, 577 Airport Boulevard, Suite 250, Burlingame, California 94010. (D,R)

312. *DISH Network, L.L.C, v. Broadband iTV, Inc.,* IPR2020-01280, Patent Trial and Appeal Board. Served as an expert for patent owner in in an *inter partes* review of U.S. Patent 9,998,791, relating to hierarchical navigation of video-on-demand television menus. Case has settled. Contact: Sal Lim, Esq., Kramer Day Alberti Lim Tonkovich & Belloli LLP, 577 Airport Boulevard, Suite 250, Burlingame, California 94010. (D,R)

313. *DISH Network, L.L.C, v. Broadband iTV, Inc.,* IPR2020-01359, Patent Trial and Appeal Board. Served as an expert for patent owner in in an *inter partes* review of U.S. Patent 9,648,388, relating to hierarchical navigation of video-on-demand television menus. Case has settled. Contact: Sal Lim, Esq., Kramer Day Alberti Lim Tonkovich & Belloli LLP, 577 Airport Boulevard, Suite 250, Burlingame, California 94010. (D,R)

314. *Justservice.net, LLC. v. Dropbox, Inc.*, Case 6:20-cv-00070-ADA (W.D. Texas). Served as an expert for Defendants in an action alleging infringement of U.S. Patents 8,126,990, 8,195,776, 8,392,542, 9,772,993, 10,387,270 and 10,472,868, relating to network-based file backup systems. Case has settled. Contact: Monica Grewal, Esq., Wilmer Cutler Pickering Hale and Dorr LLP, 60 State Street, Boston, MA 02109.

315. *Dropbox, Inc. v. Motion Offense, LLP*, Case 6:20-cv-00251-ADA (W.D. Texas). Served as an expert for declaratory judgment plaintiff Dropbox in an action relating to alleged infringement of U.S. Patents 10,013,158, 10,021,052, 10,303,353, 10,587,548, and 10,613,737, relating to file-sharing systems. At trial, all asserted claims were found not infringed, not entitled to priority to 2012, and were found invalid. Contact: Monica Grewal, Esq., Wilmer Cutler Pickering Hale and Dorr LLP, 60 State Street, Boston, MA 02109. (D,R,T)

316. *HealthPlanCRM, LLC d/b/a Cavulus v. AvMed, Inc. et al.*, Case 01-19-0002-2557 (American Arbitration Association). Served as an expert for respondents in an arbitration alleging misappropriation of trade secrets concerning a customer relationship management (CRM) platform relating to Medicare Advantage Plans. Result: all claims dismissed by arbitrator. Contact: Chris Schwing, Esq., Holland & Knight LLP, 50 N. Laura Street, Suite 3900, Jacksonville, FL 32202. (R)

317. *Talavera et al. v. Global Payments, Inc. et al.*, Case 3:21-cv-1585-TWR-AGS (S.D. Cal.). Served as an expert for defendants in an action alleging infringement of copyright in a computer program that operates storefronts for online purchase of school supplies. Contact: Matthew D. Murphey, Esq., Murphey & Murphey, 120 Vantis Drive, Suite 300, Aliso Viejo, California 92656. (R)

318. *AlphaSense Oy et al. v. Sentieo, Inc.,* Case 1:21-cv-01011-CFC/JLH-MPT (D. Del.). Served as an expert for defendant in a case alleging infringement of U.S. Patent 11,023,675, relating to a user interface for a financial document search engine. Case has settled. Contact: Jennifer Ying,

Esq., Morris, Nichols, Arsht & Tunnell, LLP, 1201 North Market Street, 16th Floor, Wilmington, DE 19899-1347. (R)

319. *Triller, Inc. v. TikTok PTE, Ltd.*, IPR2022-00179, IPR2021-00180, and IPR2021-00181, Patent Trial and Appeal Board. Served as an expert for petitioner in *inter partes* reviews of U.S. Patents 9,294,430, 9,648,132, and 9,992,232, relating to systems and methods for locating and downloading digital music to a wireless device. Review was instituted in 2022-00179 and 2022-00180; denied in 2022-00181. Case has settled. Contact: Brent Lorimer, Esq., Workman Nydegger, 60 East South Temple, Suites 1000, Salt Lake City, UT 84111. (D,R)

320. *RFCyber Corp. v. Google LLC and Google Payment Corp.*, C.A. 2:20-cv-00274-JRG (E.D. Texas). Served as an expert for Google in an action alleging infringement of U.S. Patents 6,292,657, 8,118,218, 8,448,855, 9,187,7877, 9,240,009, and 10,600,046, relating to electronic commerce payment methods. Case has settled. Contact: Heather Takahashi, Esq., Munger, Tolles & Olson LLP, 355 South Grand Avenue, Los Angeles, CA 90071.

321. *KioSoft Technologies, LLC et al. v. PayRange, Inc.*, PGR2021-00077, Patent Trial and Appeal Board. Served as an expert for patent owner in a post-grant review of U.S. Patent 10,719,833, relating to methods for authorizing payments wirelessly at vending machines. Result: claim 1 unpatentable; claims 2-27 not unpatentable. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304. (D,R)

322. *Fintiv, Inc. v. Apple, Inc.* C.A. 1:21-cv-00896-ADA (W.D. Texas). Serving as an expert for plaintiff in an action alleging infringement of U.S. Patent 8,843,125, relating to a system and method for managing a mobile wallet through a Trusted Service Manager (TSM). Defendant obtained summary judgment of non-infringement, now on appeal to the Federal Circuit. Contact: Marcus Barber, Esq., Kasowitz Benson Torres LLP, 333 Twin Dolphin Drive, Suite 200, Redwood Shores, CA 94065. (D, R)

323. *NRT Technology Corp. et al. v. Everi Holdings Inc. et al.*, C.A. 1:19-cv-00804-MN (D. Del.). Serving as an expert for Plaintiffs in an action alleging misuse of U.S. Patent 6,081,792, relating to structuring ATM and POS transactions with respect to withdrawal limits. Contact: Colby B. Springer, Esq., Polsinelli LLP (formerly at Lewis Roca Rothgerber LLP), Three Embarcadero Center, Suite 1350, San Francisco, CA 94111. (D,R)

324. *KioSoft Technologies, LLC et al. v. PayRange, Inc.*, PGR2021-00093, Patent Trial and Appeal Board. Served as an expert for patent owner in a post-grant review of U.S. Patent 10,891,614, relating to methods for authorizing payments wirelessly at vending machines. Claims 7, 11-13, 16 and 17 found not unpatentable. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304. (D,R)

325. *OANDA Corporation v. GAIN Capital Holdings Inc. et al.*, C.A. 3:20-cv-05784-ZNQ-DEA (D. N.J.). Serving as an expert for Plaintiff in an action alleging infringement of U.S. Patents

7,146,336 and 8,392,311, relating to systems and methods of online currency trading. Contact: Drew Koning, Esq., Koning Zolar LLP 169 Saxony Road, Suite 115, Encitas, CA 92024-6780. (R)

326. *AnywhereCommerce, Inc. et al. v. Ingenico, Inc. et al.,* C.A. 1:19-cv-11457-IT (D. Mass.). Served as an expert for Defendants in an action alleging infringement misappropriation of trade secrets involving card reading devices connecting to cellphones via audio jack. Result: verdict for Defendants. Contact: Jeffrey Techentin, Esq., Adler Pollock & Sheehan P.C., One Citizens Plaza, 8th Floor, Providence, RI 02903-1345. (D,R,T)

327. *Samsung Electronics Co. Ltd. v. Aire Technology Ltd,*, IPR2022-00875, Patent Trial and Appeal Board. Served as an expert for petitioner in an *inter partes* review of U.S. Patent 8,205,249, relating to a method for carrying out a secure electronic transaction. Terminated by settlement prior to institution. Contact: Daniel Tishman, Esq., Fish & Richardson, P.C., 1000 Maine Avenue, S.W., Suite 1000, Washington, DC 20024. (R)

328. *Content Square SAS v. Quantum Metric, Inc.*, IPR2022-01167, Patent Trial and Appeal Board. Served as an expert for petitioner in an *inter partes* review of U.S. Patent 11,036,823, relating to a method for capturing and replaying user interactions with a webpage through a Document Object Model (DOM) tree. Terminated by settlement. Contact: Stephen R. Smith, Esq., Cooley LLP, 1299 Pennsylvania Avenue, NW, Suite 700, Washington, DC 20004-2400. (R)

329. *Open Text Corporation et al. v. SAS C6,* C.A. 2084-cv-02578-BLS1 (Mass. Super.). Served as an expert for Defendant in an action alleging breach of a software license agreement and misappropriation of trade secrets involving enterprise content management systems. Case has settled. Contact: Matthew C. Hurley, Esq., Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C., One Financial Center, Boston, MA 02111. (R)

330. *ABG Intermediate Holdings 2, LLC at al. v. Bolt Financial, Inc.,* C.A. 22-cv-00473-IT (S.D. N.Y.). Served as an expert for Plaintiff in a case alleging breach of contract for development of an ecommerce software platform and misuse of proprietary information. Case has settled. Contact: Bill Natbony, Esq., Cadwalader, Wickersham & Taft LLP, 200 Liberty Street, New York, NY 10281.

331. *In the Matter of Certain Digital Set-Top Boxes and Systems and Services Including the Same*, USITC Inv. No. 337-TA-1315. Served as an expert for Complainant Broadband iTV, Inc. in an ITC proceeding alleging infringement of U.S. Patents 9,866,909, 9,936,240, 10,555,014, and 11,277,699, relating to hierarchical navigation of video-on-demand television menus. Case has settled. Contact: Sal Lim, Esq., Kramer Day Alberti Lim Tonkovich & Belloli LLP, 577 Airport Boulevard, Suite 250, Burlingame, California 94010. (R)

332. *Proofpoint, Inc. et al. v. Vade Secure Incorporated et al.*, Case 3:19-cv-04238-MMC (N.D. Cal.). Served as an expert for plaintiffs in an action alleging misappropriation of trade secrets and breach of employment and confidentiality agreements relating to cybersecurity technology.

Result: jury verdict for plaintiffs for $13.9 million. Contact: Sean Pak, Esq., Quinn Emanuel Urquhart & Sullivan, LLP, 50 California Street, 22nd Floor San Francisco, California 94111.

333. *Apple, Inc. v. Fintiv, Inc.,* IPR2022-00976, Patent Trial and Appeal Board. Serving as an expert for Patent Owner in an inter-partes review of U.S. Patent 9,892,386, relating to a mobile financial services system for making payments using mobile wallets. All challenged claims found unpatentable, now on appeal to the Federal Circuit. Contact: Marcus Barber, Esq., Kasowitz Benson Torres LLP, 333 Twin Dolphin Drive, Suite 200, Redwood Shores, CA 94065. (D,R)

334. *BJ's Wholesale Club Holdings, Inc. v. Walmart Apollo, LLC.,* IPR2022-01471, Patent Trial and Appeal Board. Served as an expert for Petitioner in an inter-partes review of U.S. Patent 10,121,133, relating to a method for retail self-checkout using a mobile device. Institution was denied. Contact: Michael Messinger, Esq., Vorys, Sater, Seymour and Pease LLP, 1909 K Street NW, Suite 900, Washington, DC 20006-1152. (D,R)

335. *KioSoft Technologies, LLC et al. v. PayRange, Inc.*, PGR2021-00084, Patent Trial and Appeal Board. Served as an expert for patent owner in a post-grant review of U.S. Patent 10,891,608, relating to methods for authorizing payments wirelessly at vending machines. Review was not instituted. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304.

336. *Versata Software, Inc., et al. v. Configit A/S,* Case 2:20-cv-09019-JAK-MRW (C.D. Cal.). Served as an expert for Plaintiff in an action alleging trade secret misappropriation and infringement of U.S. Patents 6,836,766 and 10,360,612, relating to product configuration systems. Case has settled. Contact: Michael Chibib, Esq., Bracewell LLP, 111 Congress Avenue, Suite 2300, Austin, TX 78701-4061 (R)

337. *Apple, Inc. v. Mozido-Corfire-Korea, Ltd.,* IPR2022-01149, Patent Trial and Appeal Board. Served as an expert for real party in interest Fintiv, Inc. in an inter-partes review of U.S. Patent 10,223,692, relating to a method for establishing a temporary payment cards on a mobile device. All challenged claims found unpatentable. Contact: Marcus Barber, Esq., Kasowitz Benson Torres LLP, 333 Twin Dolphin Drive, Suite 200, Redwood Shores, CA 94065. (D,R)

338. *Apple, Inc. v. Mozido, Inc.,* IPR2022-01150, Patent Trial and Appeal Board. Served as an expert for real party in interest Fintiv, Inc. in an inter-partes review of U.S. Patent 9,189,785, relating to a method for selecting a debit network using a scannable code. Some challenged claims found unpatentable. Claims 5, 12, and 19 found patentable. Contact: Marcus Barber, Esq., Kasowitz Benson Torres LLP, 333 Twin Dolphin Drive, Suite 200, Redwood Shores, CA 94065. (D,R)

339. *In re Xyrem (Sodium Oxybate) Antitrust Litigation,* Case 5:20-md-02966-RS (N.D. Cal.). Deposed as a fact witnesss concerning expert reports submitted in case 149, *Jazz Pharmaceuticals, Inc. v. Roxane Laboratories, Inc.*, regarding methods for controlling the distribution of sensitive drugs. Contact: Jack E. Pace III, Esq., White & Case LLP, 1221 Avenue of the Americas, New York, NY 10020 (D)

340. *Roku, Inc. v. IOENGINE, LLC,* IPR2022-01257, IPR2022-01258, Patent Trial and Appeal Board. Served as an expert for Patent Owner in inter-partes reviews of U.S. Patent 10,447,819, relating to a secure portable device implementing a plug-n-play VPN. Institution denied in both IPRs. Contact: Greg Chuebon, Esq., Dechert LLP, Three Bryant Park, 1095 Avenue of the Americas, New York, NY 10036-6797. (D,R)

341. *Beijing Meishe Network Technology Co., Ltd. v. TikTok Inc.*, C.A. 6:21-cv-00504-ADA-JCM (W.D. Texas). Serving as an expert for plaintiff in an action alleging copyright infringement and trade secret misappropriation of software for editing video and audio on mobile devices. Contact: Stephanie Wood, Esq., Cherian LLP, 8350 N. Central Expressway, Suite 1900, Dallas, TX 75206.

342. *Ivanti, Inc. v. Patch My PC, LLC*, C.A. 1:22-cv-00643-NYW-SKC (D. Col.). Served as an expert for defendant in an action alleging infringement of U.S. Patents 6,990,660, 7,823,147 and 8,407,687, relating to methods for updating software remotely over a network by using patch fingerprints. On summary judgment, all asserted claims were found paten-ineligible under 35 U.S.C. § 101. Contact: Daniel W. McDonald, Esq., Merchant & Gould P.C., Suite 220, 150 S. Fifth St., Minneapolis MN 55402. (D,R)

343. *Samsung Electronics, Co. Ltd. v. Cardware, Inc.,* IPR2023-00196, IPR2023-00210, IPR2023-00211, and IPR2023-00219, Patent Trial and Appeal Board. Served as an expert for Petitioner in inter-partes reviews of U.S. Patents 10,810,579 (IPR 196), 10,339,520 (IPRs 210, 211), and 11,176,538 (IPR 219), relating to a device for simulating a magnetic-stripe credit card. Institution was denied in IPR2023-00210; the remainder settled. Contact: Nicholas Stevens, Esq., Fish & Richardson, 60 South Sixth Street, Suite 3200, Minneapolis, MN 55402. (D,R)

344. *Snap, Inc. v. YouMap, Inc.*, IPR2022-00568, Patent Trial and Appeal Board. Served as an expert for Patent Owner in an inter-partes review of U.S. Patent 10,616,727, relating to providing location information associated with social network posts. Result: 16 substitute claims found patentable. Contact: Richard A. Catalina, Esq., Jardim, Meisner & Susser, P.C., 766 Shrewsbury Ave., Suite E-202, Tinton Falls, NJ 07724. (D,R)

345. *Everi Payments, Inc. v. Sightline Payments LLC,* IPR2022-00614, IPR2022-00663, and, IPR2022-00696, Patent Trial and Appeal Board. Served as an expert for Patent Owner in inter-partes reviews of U.S. Patents 8,708,809 (IPR 614), 8,998,708 (IPR 663), 9,196,123 (IPR 696), 9,466,176 (IPR 706), and 9,785,926 (IPR 707), relating to systems for funding casino gaming accounts also usable for non-gaming purposes. All challenged claims found unpatentable. Contact: James Murphy, Esq., Polsinelli LLP, 1000 Louisiana Street, 64 Fl, Houston, TX 77002. (D,R)

346. *SurgeTech, LLC v. Uber Technologies, Inc.,* C.A. 1:22-cv-00882-GBW-CJB (D. Del.). Serving as an expert for plaintiff in an action alleging infringement of U.S. Patents 11,334,598, 11,360,999 and 11,475,047, relating to methods for allocating and pricing transportation services based on supply, demand and performance factors. Contact: James Glass, Esq., Quinn

Emanuel Urquhart & Sullivan LLP, 51 Madison Avenue, 22nd Floor, New York, New York 10010.

347. *Samsung Electronics, Co. Ltd. v. Cardware, Inc.,* IPR2023-00314, Patent Trial and Appeal Board. Served as an expert for Petitioner in an inter-partes review of U.S. Patent 10,628,820, relating to a device for simulating a magnetic-stripe credit card. Case has settled. Contact: Nicholas Stevens, Esq., Fish & Richardson, 60 South Sixth Street, Suite 3200, Minneapolis, MN 55402. (R)

348. *Election Systems & Software, LLC v. Smartmatic USA Corporation,* 1:18-cv-01259-UNA (D. Del.). Served as an expert for plaintiff in a case alleging infringement of U.S. Patent 8,096,471, relating to a ballot marking device having an attached ballot box. The asserted claims were found ineligible under 35 U.S.C. § 101. Contact: Robert M. Evans, Jr., Esq., Lewis Rice LLC, 600 Washington Avenue, Suite 2500, St. Louis, MO 63101. (D,R)

349. *Textile Computer Systems, Inc. v. Broadway National Bank et al.,* 6:21-cv-00150-ADA (W.D. Tex.). Served as an expert for defendants in cases (including 6:21-cv-00152, 6:21-cv-00154, 6:21-cv-00156 and 6:21-cv-00157) alleging infringement of U.S. Patents 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 relating to online authentication methods. Case has settled. Contact: Jeffrey D. Blake, Esq., Merchant & Gould, 191 Peachtree Street NE, Suite 3800, Atlanta, GA 30303.

350. *Kroy IP Holdings, LLC v. Groupon, Inc.,* 1:17-cv-01405-MN (D. Del.). Served as an expert for defendant in a case alleging infringement of U.S. Patent 6,061,660, relating to online incentive and award fulfillment methods. All claims found invalid on a motion to dismiss. Contact: Ryan Phelan, Esq., Marshall, Gerstein & Borun, LLP, 233 South Wacker Drive, 300 Willis Tower, Chicago, IL 60606-6357.

351. *Underwood v. IFA Holdings, LLC dba Cygnal,* 1:21-cv-00830-ACA (N.D. Ala.). Served as an expert for defendant in a case alleging violations of the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227. Case has settled. Contact: Stephen J. Baumgarner, Esq., Maynard Cooper & Gale LLP, 1901 Sixth Ave. North, Suite 1700, Birmingham, AL 35203.

352. *BJ's Wholesale Club Holdings, Inc. v. Walmart Apollo, LLC.,* IPR2022-01528, -01561, -01563, -01564, Patent Trial and Appeal Board. Served as an expert for Petitioner in an inter-partes reviews of U.S. Patent 10,803,435, relating to a method for retail self-checkout using a mobile device. Institution was denied in 1561. In 1528, 1563, and 1564, all challenged claims were found unpatentable. Contact: Michael Messinger, Esq., Vorys, Sater, Seymour and Pease LLP, 1909 K Street NW, Suite 900, Washington, DC 20006-1152. (D,R)

353. *Samsung Electronics, Co. Ltd. v. Cardware, Inc.,* PGR2023-00012, PGR2023-00013, Patent Trial and Appeal Board. Served as an expert for Petitioner in post-grant reviews of U.S. Patent 11,328,286, relating to a device for simulating a magnetic-stripe credit card. Trial has been instituted in both cases. Case has settled. Contact: Nicholas Stevens, Esq., Fish & Richardson, 60 South Sixth Street, Suite 3200, Minneapolis, MN 55402. (R)

354. *Daedalus Blue, LLC v. Microsoft Corporation,* Case 6:20-cv-01152-ADA (W.D. Texas). Served as an expert for plaintiff in an action alleging infringement by of U.S. Patent 7,177,886, relating to reliable backup to remote servers, U.S. Patent 7,437,730, relating to scalable on-demand virtual machine deployment, U.S. Patent 8,381,209, relating to hypervisor access control mechanisms, U.S. Patent 8,572,612, relating to scaling of virtual machines in a cloud computing environment, and U.S. Patent 8,671,232, relating to policy-based data management in storage-area networks. Case has settled. Contact: Robin Curtis, Esq., Bunsow De Mory LLP, 701 El Camino Real, Redwood City, CA 94063.

355. *Ebates Performance Marketing, Inc. d/b/a Rakuten Rewards v. International Business Machines Corporation*, IPR2022-00646, Patent Trial and Appeal Board. Served as an expert for patent owner in an *inter partes* review of U.S. Patent 7,631,646, relating to single sign-on in a federated computing environment. Claims 1–4, 12–16, 18, 19 found unpatentable; claims 5–11, 17, and 20 not unpatentable. Contact: Karim Oussayef, Esq., Desmarais, LLP, 230 Park Avenue, 26th Floor, New York, NY 10169. (D,R)

356. *Roku, Inc. v. IOENGINE, LLC,* IPR2022-01551, IPR2022-01552, IPR2022-01553, IPR2022-01554, Patent Trial and Appeal Board. Served as an expert for Patent Owner in inter-partes reviews of U.S. Patent 10,972,584, relating to a secure portable device implementing a plug-n-play VPN. Institution denied in all four cases. Contact: Greg Chuebon, Esq., Dechert LLP, Three Bryant Park, 1095 Avenue of the Americas, New York, NY 10036-6797. (R)

357. *Apple, Inc. v. Fintiv, Inc.,* IPR2023-00398, IPR2023-00399, Patent Trial and Appeal Board. Serving as an expert for Patent Owner in inter-partes reviews of U.S. Patents 10,438,196 and 9,208,488, respectively, relating to an infrastructure supporting multiple mobile wallet providers. Contact: Marcus Barber, Esq., Kasowitz Benson Torres LLP, 333 Twin Dolphin Drive, Suite 200, Redwood Shores, CA 94065. (D,R)

358. *IOENGINE, LLC v. Roku, Inc.,* Case 6:21-cv-01296-ADA (W.D. Texas). Served as an expert for Patent Owner in a case alleging infringement of U.S. Patents 10,447,819 and 10,972,584, relating to a secure portable device implementing a plug-n-play VPN. Result: jury verdict of non-infringement. Contact: Greg Chuebon, Esq., Dechert LLP, Three Bryant Park, 1095 Avenue of the Americas, New York, NY 10036-6797. (D,R,T)

359. *United States v. David Gerald Minkkinen et al.,* Case 2:22-cr-00613 (D. W.Va). Serving as an expert for defendant Minkkinen in a case alleging theft of trade secrets relating to statewide unemployment insurance systems. Contact: Mike Nogay, Esq., Sellitti, Nogay & Nogay, PLLC, 3125 Pennsylvania Avenue, Weirton, West Virginia 26062. (R)

360. *Hum Industrial Technology, Inc. v. Amsted Rail Company, Inc.,* IPR2023-00538, IPR2023-00539, IPR2023-00540, Patent Trial and Appeal Board. Serving as an expert for Patent Owner in inter-partes reviews of U.S. Patents 9,365,223, 9,981,673, and 10,137,915, repectively, relating to systems for detecting anomalies in train consists and railcars. Contact: Ryan N. Miller, Esq., Fox Rothschild LLP, 2000 Market Street, 20th Floor, Philadelphia, PA 19103-3222. (R)

361. *Entain Corporate Services Ltd. et al. v. GAN (UK) Limited,* IPR2023-00027, Patent Trial and Appeal Board. Served as an expert for Patent Owner in an inter-partes review of U.S. Patent 8,821,296, relating to casino management systems for linking online and offline gaming accounts. Result: all challenged claims unpatentable. Contact: Jarrad M. Gunther, Esq., Duane Morris LLP, 30 South 17th Street, Philadelphia, PA 19103-4196. (D,R)

362. *Ex Parte Reexamination of U.S. Patent 8,762,498*, Control No. 90/015,238. Served as an expert for Unified Patents in a reexamination of U.S. Patent 8,762,498, drawn to Internet communications through a virtual domain. Contact: Michael H. Jones, Esq., Rothwell, Figg, Ernst & Manbeck, P.C., 901 New York Avenue, N.W., Suite 900 East, Washington. DC 20001. (R)

363. *FaceTec, Inc. v. iProov Ltd.*, Case 2:21-cv-02252-ART-BNW (D. Nevada). Serving as an expert for Defendant/Counterclaim Plaintiff in an action alleging infringement of U.S. Patents 10,776,471 and 11,157,606 by iProov, relating to authentication through facial recognition, and infringement of U.S. Patent 9,621,548 by FaceTec, relating to online identity validation. Contact: Ryan E. Hatch, Esq., Hatch Law, P.C., 13323 Washington Blvd., Suite 100, Los Angeles, CA 90066.

364. *Lexos Media IP, LLC v. Abt Electronics, Inc.*, Case 1:22-cv-04878 (N.D. Ill.). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patents 5,995,102, 6,118,449, and 7,975,241, relating to modifying a cursor image. Case has settled. Contact: Ken P. Kula, Esq., Buether Joe & Counselors, LLC, 1700 Pacific Avenue, Suite 4750 Dallas, Texas 75201.

365. *Lexos Media IP, LLC v. Amazon.com, Inc.*, Case 2:22-cv-00169-JRG (E.D. Texas), consolidated with *Lexos Media IP, LLC v. Target Corporation*, Case 2:22-cv-00175-JRG (E.D. Texas) and *Lexos Media IP, LLC v. Office Depot*, Case 2:22-cv-00273-JRG (E.D. Texas). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patents 5,995,102, 6,118,449, and 7,975,241, relating to modifying a cursor image. Case has settled as to all defendants. Contact: Ken P. Kula, Esq., Buether Joe & Counselors, LLC, 1700 Pacific Avenue, Suite 4750 Dallas, Texas 75201. (D,R)

366. *Lexos Media IP, LLC v. MSC Industrial Direct Co., Inc.*, Case 3:22-cv-01736-X (N.D. Texas). Serving as an expert for Plaintiff in an action alleging infringement of U.S. Patents 5,995,102, 6,118,449, and 7,975,241, relating to modifying a cursor image. Contact: Ken P. Kula, Esq., Buether Joe & Counselors, LLC, 1700 Pacific Avenue, Suite 4750 Dallas, Texas 75201.

367. *Lexos Media IP, LLC v. Nike, Inc.*, Case 2:22-cv-00311-JRG (E.D. Texas), consolidated with *Lexos Media IP, LLC v. Walmart, Inc.*, Case 2:22-cv-00175-JRG (E.D. Texas), *Lexos Media IP, LLC v. Ulta Beauty, Inc.*, 2:22-cv-00292-JRG (E.D. Texas), *Lexos Media IP, LLC v. Northern Tool and Equipment, Inc.*, 2:22-cv-00355-JRG (E.D. Texas), *Lexos Media IP, LLC v. The Gap, Inc.*, 2:22-cv-00299-JRG (E.D. Texas), and *Lexos Media IP, LLC v. CDW LLC*, 2:22-cv-00275-JRG (E.D. Texas). Served as an expert for Plaintiff in an action alleging infringement of U.S. Patents 5,995,102, 6,118,449, and 7,975,241, relating to modifying a cursor image. Case has

settled as to all defendants. Contact: Ken P. Kula, Esq., Buether Joe & Counselors, LLC, 1700 Pacific Avenue, Suite 4750 Dallas, Texas 75201. (D,R)

368. *Lexos Media IP, LLC v. Overstock.Com, Inc.*, Case 1:22-cv-02324-JAR-ADM (D. Kan.). Serving as an expert for Plaintiff in an action alleging infringement of U.S. Patents 5,995,102, 6,118,449, and 7,975,241, relating to modifying a cursor image. Contact: Ken P. Kula, Esq., Buether Joe & Counselors, LLC, 1700 Pacific Avenue, Suite 4750 Dallas, Texas 75201.

369. *CosmoKey Solutions GmbH & Co. KG v. Duo Security, Inc.*, 1:18-cv-1477 (D. Del.). Serving as an expert for plaintiff in a case alleging infringement of U.S. Patent 9,246,903, relating to online authentication using two communication channels. Contact: John Paul Padro, Esq., Goodwin Procter LLP, The New York Times Building, 620 Eighth Avenue, New York, NY 10018.

370. *United Services Automobile Association v. Truist Bank,* 2:22-cv-00291-JRG-RSP (E.D. Texas). Served as an expert for plaintiff in a case alleging infringement of U.S. Patents 9,818,090, 10,482,432, 11,182,753, 11,544,944, and 11,625,770, relating to remote check deposit. Defendant has counterclaimed, asserting infringement of U.S. Patents 7,336,813, 7,519,214, relating to determining skew in digital images, U.S. Patents 7,283,644, 7,899,210, and 9,760,797, relating to an image-based security system, and U.S. Patent 8,136,721, relating to improvements in optical character recognition. Case has settled. Contact: Anthony Rowles, Esq., Irell & Manella LLP, 1800 Avenue of the Stars, Los Angeles, CA 90067-4276.

371. *RFCyber Corp. v. Visa U.S.A., Inc.,* 6:22-cv-00697-ADA (W.D. Texas). Serving as an expert for Visa in a case alleging infringement of U.S. Patents 8,118,218, 8,448,855, 9,189,717, and 9,240,009, relating to mobile payment devices and funding electronic purses. Contact: James C. Yoon, Esq., Wilson Sonsini Goodrich & Rosati P.C., 650 Page Mill Road, Palo Alto, CA 94304-1050. (R)

372. *SitePro, Inc. v. Waterbridge Resources, LLC et al.,* 6:23-cv-00115-ADA-DTG (W.D. Texas). Serving as an expert for SitePro in a case alleging infringement of U.S. Patents 8,649,909, 9,342,078, 9,898,014, 10,488,871, 11,165,680, and 11,294,403, relating to remote control of fluid-handling devices. Contact: M. Craig Tyler, Esq., Perkins Coie LLP, 405 Colorado Street, Suite 1700, Austin, TX 78701-0089.

373. *Diogenes Limited and Colossus (IOM) Limited v. DraftKings Inc.,* 1:21-cv-01695-MN-CJB (D. Del.). Serving as an expert for DraftKings in a case alleging infringement of U.S. Patents 8,721,439, 9,117,341, 9,275,516, 9,424,716, 9,704,338, 10,970,969, 10,997,822,and 11,200,779, relating to wagering methods, in particular, offering to cash out a wager on an event before the event has terminated. Contact: Jamie R. Lynn, Esq., Baker Botts L.L.P., 700 K Street N.W., Washington, DC 20001.

374. *Truist Bank v. United Services Automobile Association,* IPR2023-00183 (PTAB). Served as an expert for Patent Owner in an inter-partes review of U.S. Patent 11,182,753, relating to remote check deposit. Case has settled. Contact: Anthony Rowles, Esq., Irell & Manella LLP, 1800 Avenue of the Stars, Los Angeles, CA 90067-4276. (R)

375. *Redmon Jeang LLC v. TurnSignl, Inc. et al.,* 0:22-cv-02749-NEB-LIB (D. Minn.). Serving as an expert for defendant in a case alleging infringement of U.S. Patents 11,443,395, 11,494,861, and 11,494,862, relating to systems and methods for contacting an attorney during a traffic stop. Contact: Mark Nelson, Esq., Barnes & Thornburg LLP, 2121 N. Pearl Street, Suite 700, Dallas, TX 75201.

376. *TurnSignl, Inc. et al. v. Redmon Jeang LLC,* IPR2024-00103, IPR2024-00104, IPR2024-00105, Patent Trial and Appeal Board. Serving as an expert for Patent Owner in inter-partes reviews of U.S. Patents 11,443,395, 11,494,861, and 11,494,862, repectively, relating to systems and methods for contacting an attorney during a traffic stop. Contact: Mark Nelson, Esq., Barnes & Thornburg LLP, 2121 N. Pearl Street, Suite 700, Dallas, TX 75201. (R)

377. *MessageBird, B.V. et al. v. Validity, Inc. ,* 1:22-cv-12116-NMG (D. Mass.). Served as an expert for defendant in a case alleging infringement of U.S. Patent 8,719,356, relating to monitoring deliverability of electronic mail. Case has settled. Contact: Jennifer Hayes, Esq., Nixon Peabody LLP, 305 D. Grand AvenueSuite 4100, Los Angeles, CA 90071-3151.

378. *Cardware, Inc. v. Samsung Electronics, Co. Ltd. et al,* 2:22-cv-00141-JRG-RSP (E.D. Texas). Served as an expert for Defendants in a case alleging infringement of U.S. Patents 10,339,520, 10,628,820, 10,810,579, 11,176,538, and 11,328,286, relating to a device for simulating a magnetic-stripe credit card. Case has settled. Contact: Nicholas Stevens, Esq., Fish & Richardson, 60 South Sixth Street, Suite 3200, Minneapolis, MN 55402.

379. *Cortex MCP, Inc. v. VISA Inc.*, 5-23-cv-05720-FB (N.D. Cal.). Serving as an expert for defendant in an action alleging infringement of U.S. Patents 9,251,531, 9,954,854, 10,749,859, and 11,329,973, all relating to tokenization methods for securing electronic credentials, e.g., in electronic payment systems. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304.

380. *VISA Inc. v. Cortex MCP, Inc. v. VISA Inc.*, IPR2024-00486, IPR2024-00487, IPR2024-00488, IPR2024-00489, and IPR2024-00490, Patent Trial and Appeal Board. Serving as an expert for petitioner in inter partes reviews of U.S. Patents 9,251,531 (IPR2024-00486, IPR2024-00487), 9,954,854 (IPR2024-00488), 10,749,859 (IPR2024-00489), and 11,329,973 (IPR2024-00490), all relating to tokenization methods for securing electronic credentials, e.g., in electronic payment systems. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304.

381. *Snap Inc v. Playvuu, Inc.,* IPR2023-00848 (PTAB). Served as an expert for Patent Owner in an inter-partes review of U.S. Patent 10,931,911, relating to compositing multimedia content. Review has been instituted. Contact: David Tsai, Esq., Pillsbury Winthrop Shaw Pittman LLP, Four Embarcadero Center, 22nd Floor San Francisco, CA 94111-5998. (R)

382. *Zigen, Inc. et al. v. Cabin Management Solutions et al.*, 4-23-cv-00210 (S.D. Texas). Serving as an expert for defendant in an action alleging misappropriation of trade

secrets relating to customized aircraft audiovisual systems. Contact: Peter Vogel, Esq., VogelITLaw, 5925 Forest Lane, Suite 136, Dallas, TX 75230.

383. *The Chosen, Inc. v. Angel Studios, Inc. v. Come and See Foundation, Inc.*, AAA 01-23-001-5829. Serving as an expert for interested party Educational Media Foundation in an action alleging software copyright infringement. Contact: Thor Y. Urness, Esq., Bradley Arant Boult Cummings LLP, Roundabout Plaza, 1600 Division Street, Suite 700, Nashville, TN 37203.

384. *AirSlate, Inc. v. Inkit, Inc.*, 1:23-cv-01307-RGA-SRF (D. Del.). Serving as an expert for defendant in a case alleging infringement of U.S. Patent 11,449,815, relating to automating document workflows. Contact: John M. Hintz, Esq.., Maynard Nexsen PC, 551 Fifth Avenue, The Fred F. French Building, Suite 1600, New York, NY 10176. (R)

385. *CSC Serviceworks, Inc.. v. PayRange, Inc.*, IPR2023-01186, Patent Trial and Appeal Board. Served as an expert for patent owner in a post-grant review of U.S. Patent 8,856,045, relating to methods for authorizing payments wirelessly at vending machines. Case has settled. Contact: Matthew Argenti, Esq., Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304. (R)

Legislative Testimony

Testimony before the Texas Legislature concerning electronic voting, Austin, Texas, 1987. Result: passage of the Texas Electronic Voting Law.

Invited testimony before the British House of Lords, Subcommittee B of the European Union Committee, April 20, 2000. Subject: European regulation of eCommerce.

Testimony before the Pennsylvania Legislature State Government Committee concerning electronic voting, Philadelphia, March 10, 2004.

Testimony before the United States Commission on Civil Rights concerning electronic voting, Washington, DC, April 9, 2004.

Testimony before the U.S. House of Representatives Committee on Science concerning voting system certification, Washington, DC, June 24, 2004.

Testimony before the U.S. House of Representatives Committee on House Administration concerning voting system security, Washington, DC, July 7, 2004.

Testimony before the U.S. House of Representatives Committee on Government Reform concerning electronic voting technology, Washington, DC, July 20, 2004.

Testimony on DREs and paper trails before the Virginia Legislature Study Commission on Voting System Certification and Security, Richmond, VA, August 16, 2004.

Testimony before the Election Assistance Commission, Technical Guidelines Development Committee, Subcommittee on Computer Security and Transparency, Gaithersburg, MD, Sept. 20, 2004.

Testimony before the House Ways and Means Committee of the Maryland General Assembly on voting machine paper trails, Annapolis, MD, December 7, 2004.

Testimony before the U.S. House of Representatives Committee on House Administration concerning paper trails, Washington, DC, September 28, 2006.

Testimony before the U.S. Election Assistance Commission concerning the Voting System Testing and Certification Program, Washington, DC, October 26, 2006.

Testimony before the Georgia State Board of Elections, Powder Springs, GA, December 21, 2007.

Testimony before the Maryland House of Delegates Ways and Means Committee, Annapolis, MD, January 18, 2007.

Testimony before the U.S. Senate Committee on Rules and Administration on the Ballot Integrity Act of 2007, Washington, DC, July 25, 2007.

Arbitration

Dr. Shamos has served as an arbitrator in computer-related disputes for the American Arbitration Association.

Electronic Voting

Dr. Shamos has served as an examiner of electronic voting systems and consultant on electronic voting.

Member, Sarasota Source Code Audit Task Force, Florida Secretary of State (2007-2008)

Consultant to the Pennsylvania Secretary of the Commonwealth (2004-).

Consultant to the Massachusetts Secretary of the Commonwealth (2006).

Project SERVE Security Peer Review Group (2003).

Attorney General's Designee for electronic voting examinations, State of Texas (1987-2000).

Statutory Examiner for electronic voting, Commonwealth of Pennsylvania (1980-1996).

Consultant to Montgomery County, Pennsylvania (1996).

Consultant to the Secretary of State of Nevada (1996).

Consultant to the Delaware Legislature (1989).

Consultant to the Secretary of State of West Virginia (1984).

Business Experience

President, Expert Engagements LLC, expert witness firm (2003-present).

President, Unus, Inc., database publishing software (formerly Unilogic, Ltd.) (1990-1992)

President, Notifax Corporation (1989-1994). Automated notification by facsimile.

President, Lexeme Corporation (1984-87), software language translation products.

Managing Partner, Shamos and Tchen (1978-82), computer consulting firm.

Supervisory Programmer, National Cancer Institute (1970-72), while a commissioned officer in the United States Public Health Service (O-3).

Associate Engineer, IBM Corporation (1968-70) (Components Division), design of manufacturing information systems.

Consulting

Morgan Stanley Dean Witter (2000-2002) (now Morgan Stanley).

McKinsey & Co. (1999-2001).

Bell Atlantic Corporation (1999-2008) (now Verizon).

LG-CNS, South Korea (2002-2004). Project to automate the Korean court system.

Directorships

Unilogic, Ltd. (1979–87) (later Unus, Inc. d/b/a Cygnet Publishing Technologies, 1987-2013). Database publishing software.

The Billiard Archive (1983–), also Curator. Historical nonprofit foundation.

Lexeme Corporation (1984-1987). Computer source language translation.

Notifax Corporation (1989-1994)

Insurance Technology Corporation (1992–1995). IT consulting for the insurance industry.

Personal Data

Date of birth: April 21, 1947.

Married to Julie Shamos (formerly Julie Van Allen), August 12, 1973.

Children: Josselyn (born May 20, 1982), Alexander (born August 3, 1984).

Grandchildren: Harlow Elizabeth Crane (born April 9, 2010), Bishop Moses Crane (born July 13, 2012), Amelia Eleanor Shamos (born April 17. 2019), Sophia Anastasia Shamos (born March 14, 2021)

Military Status: Veteran (Commissioned Officer, U.S. Public Health Service, 1970-72).

Contact Information

Contact should be by email. Letters and packages should be sent to the Home Address:

Home Address:
605 Devonshire Street
Pittsburgh, PA 15213-2904
Home Telephone: 412-681-8398
Home Fax: 412-681-8916

Office Address:
6707 Gates Hillman Complex
5000 Forbes Avenue
Carnegie Mellon University
Pittsburgh, PA 15213
Office Telephone: 412-268-8193
Office Fax: 412-268-6298
Email: shamos@cs.cmu.edu

Publications

Google Scholar citations. Erdös number = 3: Erdös -> {Daniel Kleitman, Patrick O'Neill, Joel Spencer} -> Albert Meyer -> Shamos

SCIENCE

Books

1. *Computational Geometry: An Introduction*, with F. P. Preparata. Springer-Verlag (1985, revised ed., 1991), 390 pp. ISBN 0387961313. According to CiteSeer in 2012, this is the 93rd most cited work in the field of computer science.

2. *Вычислительная геометрия: введение*. Russian translation of "Computational Geometry: An Introduction." Moscow: Mir Publishers (1989). ISBN 5030010416.

3. *Keisan kikagaku nyumon*. Japanese translated by T. Asano and T. Asano of *Computational Geometry: An Introduction*, with F. P. Preparata. Soken Shuppan (Jul. 1992). ISBN 4795263213.

4. *Handbook of Academic Titles*. 193 pp. (Jan. 2011). An encyclopedia of various academic designations used at over 1000 colleges and universities in the United States.

5. *Geometria obliczeniowa. Wprowadzenie*. Polish translation of "Computational Geometry: An Introduction." Warsaw: Helion (2003) 392 pp. ISBN 83-7361-098-7.

6. *Shamos's Catalog of the Real Numbers*. A list, patterned after Sloane & Plouffe, The Encyclopedia of Integer Sequences, Academic Press (1995). Over 10,000 interesting real numbers arranging in lexical order by decimal expansion, with accompanying formulas.

Book Chapters

1. "Privacy and Public Records." Chapter 16 in *Personal Information Management*, Jones & Teevan, eds., Univ. of Washington Press (2007), ISBN978-0-295-98737-8.

Articles

1. "On the Piezoelectric Effect in Bone," with M. H. Shamos and L. S. Lavine. *Nature* **197**:81 (1963).

2. "An Absorber Theory of Acoustical Radiation," with M. A. Tavel. *Journal of the Acoustical Society of America* **54**:46–49 (1973).

3. "Problems in Computational Geometry." Unpublished book manuscript (1974, revised 1977). Distributed in photocopy.

4. "Geometric Complexity." *Proceedings of the Seventh Annual ACM Symposium on Automata and Theory of Computation* (May 1975) 224–233.

5. "Closest-point Problems," with D. J. Hoey. *Proceedings of the Sixteenth IEEE Symposium on Foundations of Computer Science* (Oct. 1975) 151–162.

6. "Divide and Conquer in Multidimensional Space," with J. L. Bentley. *Proceedings of the Eighth Annual ACM Symposium on Automata and Theory of Computing* (May 1976) 220–230.

7. "Geometric Intersection Problems," with D. J. Hoey. *Proceedings of the Seventeenth Annual IEEE Symposium on Foundations of Computer Science* (Oct. 1976) 208–215.

8. "Lower Bounds from Complex Function Theory," with G. Yuval. *Proceedings of the Seventeenth Annual IEEE Symposium on Foundations of Computer Science* (Oct. 1976) 268–273.

9. "Geometry and Statistics: Problems at the Interface." In *Algorithms and Complexity: New Directions and Recent Results*, J. F. Traub, ed., Academic Press (1976) 251–280.

10. "Divide and Conquer for Linear Expected Time," with J. L. Bentley. *Information Processing Letters* 7 (1977) 87–91.

11. "A Problem in Multivariate Statistics: Algorithm, Data Structure, and Applications," with J. L. Bentley. *Proceedings of the Fifteenth Allerton Conference on Communications, Control and Computers* (Sep. 1977) 193–201.

12. "Optimal Algorithms for Structuring Geographic Data," with J. L. Bentley. *Proceedings of the Harvard Conference on Topological Data Structures for Geographic Information Systems* (Oct. 1977) 43–51.

13. "Computational Geometry." Ph.D. Thesis, Yale University (1978). University Microfilms, Ann Arbor, MI.

14. "Time and Space," with A. R. Meyer. In *Perspectives on Computer Science*, A. K. Jones, ed. Academic Press (1978).

15. *Combinatorics on Graphs I: Graph Polynomials*. Unpublished book manuscript (1978).

16. "Robust Picture Processing Operators and Their Implementation as Circuits." *Proceedings of the Fall 1978 Workshop on Image Processing*, Carnegie Mellon University (1978).

17. "A practical system for source language translation," with T. R. Kueny and P. L. Lehman. *Proceedings of the National Conf. on Software Reuseability and Maintainability*, pp. B-1 – B-12, Washington, DC (Sep. 1986).

18. "The Early Years of Computational Geometry – A Personal Memoir." *Advances in Discrete and Computational Geometry* (B. Chazelle, J. E. Goodman, and R. Pollack, eds.), *Contemporary Mathematics*, Amer. Math. Soc., Providence (1998).

19. "A Multiparty Computation for Randomly Ordering Players and Making Random Selections," with Latanya Sweeney. Carnegie Mellon Univeristy School of Computer Science Technical Report CMU-ISRI-04-126 (July 2004)

20. *Overcounting Functions*. A systematic method of transforming certain multiple summations into single summations, with new number-theoretic results.

21. *Property Enumerators and a Partial Sum Theorem*. A new result allowing rapid symbolic evaluation of certain types of double summations.

DIGITAL LIBRARIES

Articles

1. "Machines as readers: a solution to the copyright problem." J. Zhejiang Univ. Science 6A, 11, pp. 1179-1187 (Nov. 2005).

Book Chapters

1. "The Universal Digital Library: Intelligent Agents and Information on Demand," with Raj Reddy. Chapter 6 in Emerging Communication Technologies and the Society, by N. Balakrishnan, Indian National Science Academy (2000). ISBN 81-7319-341-X.

Reports

1. "Japanese Digital Information Policy, Intellectual Property and Economics," in "Digital Information Organization in Japan," International Technology Research Institute (1999).

ELECTRONIC VOTING

Books

1. "Glossary of Electronic Voting."

Articles

2. "Voting System Certification — An Examiner's View." Invited paper presented at the Election Center Conference, Reno, Nevada (Sep. 1989).

3. "Electronic Voting — Evaluating the Threat." Proc. Third ACM Conf. on Computers, Freedom & Privacy, San Francisco, CA (Mar. 1993).

4. "Paper v. Electronic Voting Records — An Assessment." Proc. 14th ACM Conf. on Computers, Freedom & Privacy, Berkeley, CA (Apr. 2004).

5. "Evaluation of Voting Systems," with P.L. Vora, B. Adida, R. Bucholz, D. Chaum, D. Dill, D. Jefferson, D. Jones, W. Lattin, A. Rubin and M. Young, Commun. ACM 47(11):144 (2004).

6. "Voting as an Engineering Problem." *The Bridge* (publication of the National Academy of Engineering), Summer 2007, pp. 35-39.

7. "Realities of E-Voting Security," with A. Yasinsac. IEEE Security and Privacy 10:5 (Sep/Oct 2012), pp. 16-17. Also guest editor of that issue, devoted to E-voting Security.

8. "Why our voting systems are safe." Op-ed in the Pittsburgh Post-Gazette, Dec. 31, 2016.

Published Reports

9. "Software and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware," with Yasinsac et al., February 23, 2007. Review commissioned by the Secretary of State of Florida to investigate irregularities in the Florida Congressional District 13 election of 2006.

BILLIARDS

Books

1. *Pool.* New York: Mallard Press division of Bantam-Doubleday-Dell Promotional Book Company (Aug. 1991). 128 pp. ISBN 0-7924-5310-7.

2. *Le billard et le billard américain*. Paris: Minerva, 1992, reprinted 1997. 128 pp. Translation by Jean-Yves Prate of the author's American book, *Pool*. ISBN 2–8307–0160–7 (1992), 2-8814-3135-6 (1997).

3. *The Illustrated Encyclopedia of Billiards*. New York: Lyons & Burford (1993). 310 pp. ISBN 1-55821-219-1.

4. *Pool Snooker Carambola*. Padua: Facto Edizioni (1993). 128 pp. Italian translation of *Pool*. Translated by Elisabetta Bezzon. ISBN 88-85860-20-6. The first English-language billiard book ever published in Italian.

5. *Pool*. New York: Friedman/Fairfax (Jun. 1994). 128 pp. ISBN 1-56799-061-4. Paperback edition of the author's 1991 *Pool*.

6. *Shooting Pool: The People, the Passion, the Pulse of the Game*, with photographs by George Bennett. New York: Artisan (Jun. 1998). 144 pp. ISBN 1-885183-95-X. A photographic survey of pool in the U.S. in 1997. A Book-of-the-Month Club bonus selection (Fall, 1998).

7. *Setting the Stage for Fifty Years*. Coralville, IA: Billiard Congress of America (Jun. 1998). 88 pp. A history of the Billiard Congress of America.

8. *The New Illustrated Encyclopedia of Billiards*. New York: Lyons Press (1999). 320 pp. ISBN 1-55821-797-5. An expanded and revised edition of *The Illustrated Encyclopedia of Billiards*.

9. *The Complete Book of Billiards*. New York: Gramercy Books (2000). 306 pp. ISBN 0-517-20869-5. Reissue of author's 1993 *The Illustrated Encyclopedia of Billiards*.

In Preparation

SCIENCE

Articles

1. *A Graph-Theoretic Model of Electronic Payment Systems*, with Michael Trick.

LAW

Books

1. *A Dictionary of American Intellectual Property* (1995).

Invited Talks

ELECTRONIC COMMERCE

"The Future of eCommerce." Presentation to the Association for Corporate Growth, Pittsburgh, PA (Dec. 2001).

"The U.S., Korea and the Internet Bubble." Korea International Trade Association (Seoul, July 2003).

"Electronic Judiciary Services in the United States." Address at the Supreme Court of Korea (Dec. 2004).

"eGovernment in the United States." Public address at the University of Hong Kong (Feb. 2005).

"Global SCM as a Cross-Border eCommerce Model," Korea International Trade Association, Seoul, Korea (Mar. 2007).

"Innovate or Die." Invited talk at the Verizon Leadership Meeting, Morristown, NJ (Jun. 2007).

"A Formula for Innovation." Public address at the University of Hong Kong (Feb. 2008).

"Ask My Robot: How Computers Answer Questions." University of Hong Kong (Feb. 2013).

"How Bitcoin Works: A Non-Technical Introduction." University of Hong Kong (Mar. 2014).

"What's a Bitcoin? A Non-Technical Introduction." Carnegie Mellon University (Oct. 2014).

COMPUTER SCIENCE

"Surprises in Experimental Mathematics." Carnegie Mellon University Mathematics Seminar (Feb. 2002).

"Learning by Doing or Learning by Listening?" University of Hong Kong (Feb. 2007).

"Discoveries in Experimental Mathematics." University of Hong Kong (Feb. 2009).

"How Did It (Computational Geometry) Start?" Keynote address at the 20th Canadian Conference on Computational Geometry, Montreal, Canada (Aug. 2008).

"The Internet of Everything." University of Hong Kong (Mar. 2015).

"How Do Driverless Cars Work?" University of Hong Kong (Mar. 2017).

"How Machines Learn (Without Being Taught)." University of Hong Kong (Feb. 2018).

"What is Quantum Computing All About?" University of Hong Kong (Feb. 2019).

SCIENCE AND LAW

"Digital Property in the 21st Century." Keynote address for the Spring Meeting of the American Intellectual Property Law Association, Pittsburgh, PA (May 2000). View slides.

"Who Owns This Algorithm?" Carnegie Mellon University (Nov 1991); Microelectronics and Computer Corporation (Jan. 1992); Univ, of Texas at Austin (Jan. 1992); UCLA (Feb. 1992).

"New Computer Technology and Its Application to Worker's Compensation." Forum IV, Newport Beach, CA (Feb. 1992).

"The Office of the Future, If There Is One." 1994 IAIABC Conf., Pittsburgh, PA (Sep. 1994).

"The Fringes of Infringement." University of Texas, Austin, TX (Sep. 1995).

"The Arts and the Internet." Allegheny County Bar Association Continuing Legal Education course (June 26, 1996).

"The Universal Information Resource." Inventing the Future, Symposium in Honor of Raj Reddy's 60th Birthday, Carnegie Mellon University, Pittsburgh, PA (May 1998).

"The Universal Library." University of Texas at Austin (Sep. 1998)

"The Universal Library and Its Role in Scientific Information." Keynote address to the RNA Society symposium on Emerging Sources of RNA Information, Arlington, VA (Dec. 8, 1998).

"Digital Property in the 21st Century." Luncheon address to the American Intellectual Property Law Association, Pittsburgh, PA (May. 2000).

"Copyright Protection and Distance Learning." Hong Kong Intellectual Property Office (Feb. 2002).

"The Universal Dictionary." Address at International Institute of Information Technologies (IIIT), Hyderabad, India (Jan. 2003).

"The Million Book Projects." Public address at the University of Hong Kong (Jan. 2003).

"Mathematics and the Privacy Laws." ALADDIN Workshop on Privacy in D.A.T.A., Pittsburgh, PA (Mar. 2003).

"Machines as readers: a solution to the copyright problem." 1st Int'l Conf. on Universal Digital Library, Hangzhou, China (Nov. 2005).

"Your Books Might Cost More Now: The Role of the Expert in Software Patent Litigation." University of Hong Kong (Feb. 2006).

"University Technology Transfer: How to Fix It." Asia Conference on Technology Transfer (ACTT) 2006, Seoul, S. Korea (Mar. 2006).

"How Big a Problem is Copyright"? USAIN Conference, Cornell University, Ithaca, NY (Oct. 2006).

"Digital Ownership." 2d Intl. Conf. on Universal Digital Library, Alexandria, Egypt (Nov. 2006).

"Google and the Death of Books." University of Hong Kong (Feb. 2010).

"FaceWars." (About the lawsuit between Facebook and the Winkelvoss twins). University of Hong Kong (Feb. 2011).

"Swiping the iPhone: Billions Lost With the Stroke of a Pen." University of Hong Kong (Feb. 2012).

"Global Phone Wars: Apple v. Samsung." University of Hong Kong (Mar. 2016).

ELECTRONIC VOTING

"Voting System Certification — An Examiner's View." Election Center Conference, Reno, Nevada (Sep. 1989).

"Electronic Voting — Evaluating the Threat." Third Conf. on Computers, Freedom and Privacy, San Francisco, CA (Mar. 1993).

"What's Happing in Florida?" Carnegie Mellon University (Nov. 2001)."

"Electronic Voting: The Technology of Democracy." Hong Kong University (Feb. 2004).

"Theory v. Practice in Electronic Voting." DIMACS (Rutgers Univ., May 2004).

"HAVA: Are We Ready?" Panel at the League of Women Voters National Convention, Washington, DC (Jun. 2004).

"Testing Voting Machines." Panel at the American Enterprise Institute, Washington, DC (Jun. 2004).

"Electronic Voting: Promise and Peril." Talk at the Moritz College of Law, Ohio State University (Sep. 2004).

"Is e-voting ready for prime time: Legal and technical issues regarding the upcoming Presidential election." Panel at John Marshall Law School (Chicago, IL, Oct. 2004).

"Is Electronic Voting Reliable?" Talk to the Kiwanis Club of Dubuque, Iowa (Feb. 2005).

"The Top Ten Problems in Practical Electronic Voting." Int'l Workshop on Mathematics and Democracy, Ettore Majorana Centre, Erice, Sicily (Sept. 2005).

"Why Don't We Have Paper Trails in Pennsylvania?" Carnegie Mellon Univ. CyLab Seminar, Pittsburgh, PA (Jan 2006).

"Paper Trails and the Pennsylvania Certification Process." County Commissioners Association of Pennsylvania 2006 Spring Conference, Harrisburg, PA (Mar. 2006).

"The 2006 Elections: Are We Ready?" Panel at the American Enterprise Institute, Washington, DC (Sept. 2006).

"What's Right with Electronic Voting?" University Lecture Series, Carnegie Mellon University (Oct. 12, 2006).

"What Happened in Yesterday's Election?" Center for Research on Computation and Society, Harvard University (Nov. 8, 2006).

"What Happened in Sarasota County"? Council on Government Ethics Laws, New Orleans, LA (Dec. 6, 2006).

"What Happened to 18,000 Votes? Results of the Sarasota Source Code Audit." Carnegie Mellon University (Apr. 16, 2007).

"Opscan Voting: The Good, the Bad and the Ugly." Florida State Association of Supervisors of Elections, Destin, Florida (May 24, 2007).

"Voting Machine Fraud." University of Pittsburgh (Nov. 11, 2008)

EXHIBIT 1003
Declaration of Dr. Michael I. Shamos
("Shamos Decl.")

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Alkhatib *et al.*	§	Attorney Docket No.: IVI785
	§	
U.S. Patent 7,949,785	§	
	§	
Issue Date: May 24, 2011	§	Customer No.: 165774
	§	
Filing Date: March 31, 2003	§	
	§	
For: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM	§	
	§	
	§	

DECLARATION OF DR. MICHAEL I. SHAMOS
IN SUPPORT OF UNIFIED PATENTS LLC'S REQUEST FOR *EX PARTE* REEXAMINATION OF U.S. PATENT NO. 7,949,785

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE 1
TABLE OF CONTENTS 1
I. BACKGROUND AND QUALIFICATIONS 2
II. RELEVANT LEGAL STANDARDS 3
A. Analogous Art 4
B. Combining Known Elements in the Art, Common Sense 4
C. Teaching Away 6
D. Secondary Considerations 6
E. Incorporation by Reference 7
F. Claim Construction 7
III. OPINION 8
A. Level of Skill of a Person Having Ordinary Skill in the Art 8
B. Summary of My Opinions 9
C. Summary of the '785 Patent 9
D. Summary of the Prosecution History 13
E. Ground 1: *Leung* in view of *Forslöw* and *Mehta* 17
1. Overview of Leung 17
2. Overview of Forslöw 19
3. Overview of Mehta 21
4. Motivation to Combine Leung with Forslöw and Mehta 22
IV. CONCLUSION 24

UNIFIED PATENTS EXHIBIT 1003
Page 2 of 25

AA/SWA Ex. 1015, p.214 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

I. BACKGROUND AND QUALIFICATIONS

1. My qualifications are set forth in my curriculum vitae, a copy of which is attached as Appendix A to this Declaration. As set forth in my curriculum vitae (Ex. 1004):

2. I hold the title of Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. I am a member of two departments in that School, the Software and Societal Systems Department and the Language Technologies Institute. I was a founder and Co-Director of the Institute for eCommerce at Carnegie Mellon from 1998-2004 and from 2004-2018 was Director of the eBusiness Technology graduate program in the Carnegie Mellon University School of Computer Science. I am now the Director of the M.S. in Artificial Intelligence and Innovation program at Carnegie Mellon.

3. I received an A.B. (1968) from Princeton University in Physics; an M.A. (1970) from Vassar College in Physics; an M.S. (1972) from American University in Technology of Management, a field that covers quantitative tools used in managing organizations, such as statistics, operations research and cost-benefit analysis; an M.S. (1973), an M.Phil. (1974) and a Ph.D. (1978) from Yale University in Computer Science; and a J.D. (1981) from Duquesne University.

4. I have taught graduate courses at Carnegie Mellon in Electronic Commerce, including eCommerce Technology, Electronic Payment Systems, Electronic Voting and eCommerce Law and Regulation, as well as Analysis of Algorithms. Since 2007, I have taught an annual course in Law of Computer Technology. I currently also teach Artificial Intelligence and Future Markets.

5. I am also Visiting Professor at the University of Hong Kong. Since 2001, I have taught an annual graduate course there entitled Electronic Payment Systems. This is one of only a handful of graduate courses in the world on the subject of electronic payments.

6. I am the author and lecturer in a 24-hour video course on Internet protocols and have taught computer networking, wireless communication and Internet architecture since 1999. I also delivered a course for McKinsey & Company consultants on Mobile Communication.

7. From 1979-1987, I was the founder and president of two computer software development companies in Pittsburgh, Pennsylvania, Unilogic, Ltd. and Lexeme Corporation.

8. I am a named inventor on the following five issued patents relating to electronic

UNIFIED PATENTS EXHIBIT 1003
Page 3 of 25

AA/SWA Ex. 1015, p.215 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

commerce: U.S. Patent Nos. 7,330,839, 7,421,278, 7,747,465, 8,195,197 and 8,280,773.

9. I am an attorney admitted to practice in Pennsylvania and have been admitted to the Bar of the U.S. Patent and Trademark Office since 1981. I have not been asked to offer any opinions on patent law in this proceeding.

10. I have previously testified in a large number of cases concerning computer technology. My curriculum vitae in Exhibit 1004 contains a list of cases in which I have testified in the last ten years.

II. RELEVANT LEGAL STANDARDS

11. I am not acting as an attorney in this matter; I am a technical expert and do not offer any legal opinions. However, for the purposes of this Declaration, I have been informed about certain legal principles regarding patentability and related matters under United States patent law by Petitioner's counsel, which I have applied in performing my analysis and arriving at my technical opinions in this matter.

12. I understand that a claim is invalid if it is anticipated or obvious. I understand that anticipation of a claim requires that all elements of a claim must be disclosed, expressly or inherently, in a single prior art reference, arranged as in the claim. Requester's counsel has informed me that for a claimed element to be inherently present, the prior art need not expressly disclose the element, so long as the claimed element necessarily flows from a disclosure in the prior art.

13. I am informed that a person cannot obtain a patent on an invention if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art (POSITA) at the time of the invention. I am informed that a conclusion of obviousness may be founded upon more than a single item of prior art. I am also informed that obviousness is determined by evaluating the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the claim at issue, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations of non-obviousness. In addition, the obviousness inquiry should not be done in hindsight. Instead, the obviousness inquiry should be done through the eyes of a person having ordinary skill in the art at the time of the alleged invention.

UNIFIED PATENTS EXHIBIT 1003
Page 4 of 25

AA/SWA Ex. 1015, p.216 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

14. In considering whether certain prior art renders a particular patent claim obvious, I am informed that one must consider the scope and content of the prior art, examples of which include disclosures in patents, trade publications, journal articles, conference papers, industry standards, product literature and documentation, texts describing competitive technologies, requests for comment published by standard setting organizations, and materials from industry conferences.

15. I am informed that for a patent claim to be found obvious, the proper perspective to consider is that of a person having ordinary skill in the art at the time of the alleged invention. I am informed that the factors to consider in determining the level of ordinary skill in the art include (1) the educational level and experience of people working in the field at the time the invention was made, (2) the types of problems faced in the art and the solutions found to those problems, and (3) the sophistication of the technology in the field.

A. Analogous Art

16. I am informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be "analogous art" to the claimed invention. I am informed that a reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). In order for a reference to be "reasonably pertinent" to the problem, it must logically have commended itself to an inventor's attention in considering his/her problem. In determining whether a reference is reasonably pertinent, one should consider the problem faced by the inventor, as reflected either explicitly or implicitly, in the specification. I believe that all of the references I considered in forming my opinions in support of the Request are well within the range of references a person having ordinary skill in the art would have consulted by the time of the invention to address the type of problems described in the specification and addressed by the claims being challenged ("Challenged Claims").

B. Combining Known Elements in the Art, Common Sense

17. I am informed that, in order to establish that a claimed invention was obvious based on a combination of prior art elements, a clear articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I am informed that, under the U.S. Supreme Court's *KSR* decision, a combination of multiple items of prior art renders a patent claim obvious when there was an apparent reason for a person having ordinary skill at the time of the

UNIFIED PATENTS EXHIBIT 1003
Page 5 of 25

AA/SWA Ex. 1015, p.217 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

invention to combine or modify the prior art. I am informed that such reasons may include, but are not limited to, one or more of the following rationales: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

18. I am informed that the test for obviousness is *not* whether the features of a secondary reference may be *bodily incorporated* into the structure of the primary reference, but rather whether one of skill in the art would have been motivated to combine the teachings of the prior art references to achieve the claimed invention. Nevertheless, I am informed that an invention that is a combination of prior art must do more than yield predictable results to be non-obvious and that, even where one or more motivations to combine exist, claims are not necessarily obvious unless a person having ordinary skill in the art would have had a reasonable expectation of success in implementing or applying the proposed combination at the time of the invention.

19. I also am informed that in conducting an obviousness analysis, a precise teaching directed to the specific subject matter of the challenged claim need not be sought out because it is appropriate to take account of the inferences and creative steps that a POSITA would employ. In other words, the prior art need not be directed towards solving the same specific problem as the problem addressed by the patent. Further, the individual prior art references themselves need not all be directed towards solving the same problem. The prior art considered can be directed to any need or problem known in the field of endeavor at the time of invention and can provide a reason for combining the elements of the prior art in the manner claimed. Common sense teaches that familiar items may have obvious uses beyond their primary purposes, and a POSITA will often have been able to fit the teachings of multiple prior art references like pieces of a puzzle. I am informed that, under the *KSR* standard, common sense is important and should be considered in assessing obviousness.

UNIFIED PATENTS EXHIBIT 1003
Page 6 of 25

AA/SWA Ex. 1015, p.218 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

20. I also am informed that the fact that a particular combination of prior art elements was "obvious to try" may indicate that the combination was obvious even if no one attempted the combination. If the combination was obvious to try (regardless of whether it was actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than innovation. I am further informed that in many fields there may be little discussion of obvious techniques or combinations, and it often may be the case that market demand, rather than scientific literature or knowledge, will drive the design of an invention. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a POSITA has good reasons to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation, but of ordinary skill and common sense.

C. Teaching Away

21. I am informed that it is improper to combine references if the references teach away from their combination. I am informed that a reference may be said to teach away when a POSITA, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the patent applicant. In general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the patentee. I am informed that a reference teaches away, for example, if (1) the combination would produce a seemingly inoperative device, or (2) the references leave the impression that the product would not have the property sought by the patentee. However, I also am informed, that a reference does not teach away if it merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into the invention claimed. Further, a POSITA will often appreciate that different courses of action often have simultaneous advantages and disadvantages, and I am informed that the existence of such does not necessarily obviate a motivation to combine.

D. Secondary Considerations

22. I am informed that even if a *prima facie* case of obviousness is established, the final determination of obviousness must also consider "secondary considerations" if presented. In most instances, the patentee raises these secondary considerations of non-obviousness. In that context, the patentee argues an invention would not have been obvious in view of these considerations, which include: (a) commercial success of a product due to the merits of the claimed invention; (b)

UNIFIED PATENTS EXHIBIT 1003
Page 7 of 25

AA/SWA Ex. 1015, p.219 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

a long-felt, but unsatisfied need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) lack of independent simultaneous invention within a comparatively short space of time; (h) teaching away from the invention in the prior art.

23. I am further informed that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be based on prior art features. The establishment of a nexus is a question of fact. For example, if commercial success of products allegedly embodying the claims is presented as a secondary indicium of non-obviousness, the patent owner must show that such success is due to features of the claimed invention, and not features unrelated to the claimed invention or that already existed in the prior art.

24. It does not appear that Patent Owner has previously offered any secondary considerations of non-obviousness during prosecution, and I am unaware of any offered since that time. However, in my opinion the clear teachings of the prior art herein and discussed in the Request would likely overcome such "secondary considerations," if any were offered.

E. Incorporation by Reference

25. I am informed that instead of repeating some information contained in another document, an application for patent may attempt to incorporate the content of another document or part thereof by reference to the document in the text of the specification. I understand that this means the information incorporated is as much a part of the application as filed as if the text were repeated in the application and should be treated as part of the text of the application.

F. Claim Construction

26. I am informed that in performing an obviousness analysis, it is necessary to understand the scope of the claims. I am also informed that the first step in an unpatentability analysis, therefore, involves construing the claims. Second, the construed claim language is then compared to the disclosures of the prior art.

27. I am informed that claims are generally given their broadest reasonable interpretation as understood by a POSITA, in light of the patent specification. I am informed that, for the purposes of claim construction, while expert testimony may be helpful to provide background on the technology at issue, to explain how an invention works, to ensure an

UNIFIED PATENTS EXHIBIT 1003
Page 8 of 25

AA/SWA Ex. 1015, p.220 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

understanding of the technical aspects of the patent is consistent with that of a POSITA, or to establish that a particular term in the patent had a particular meaning in the pertinent field at the time of the invention, the testimony from a technical expert is generally less reliable than the patent itself and its prosecution history in determining the meaning of the claim terms, and it is not the role of technical experts to supplant the Examiner in applying principles of claim interpretation. However, the information that I provide in my Declaration sheds light on the technology at issue in this reexamination and, hopefully, provides the adjudicators with an understanding of certain pertinent technical aspects that a POSITA would have appreciated at the time of the '785 Patent's alleged invention. For the purposes of this proceeding, I have applied the broadest reasonable interpretation when analyzing the prior art and the claims.

III. OPINION

A. Level of Skill of a Person Having Ordinary Skill in the Art

28. I was asked to provide my opinion as to the level of skill of a person having ordinary skill in the field of the '785 Patent at the time of the claimed invention, which I have been instructed to assume is March 31, 2003. In determining the characteristics of a hypothetical POSITA, I was told to consider several factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the education level of active workers in the field. I also placed myself back in the time frame of the claimed invention and considered the colleagues with whom I had worked at that time.

29. In my opinion, the level of ordinary skill in the art that one would need in order to have the capability of understanding the scientific and engineering principles applicable to the '785 Patent is (i) a Bachelor's degree (or higher degree) in computer science or equivalent and (ii) at least two years of experience working in the field of virtual networking. Additional industry experience or technical training may offset less formal education, while advanced degrees or additional formal education may offset lesser levels of professional experience.

30. Based on my education, training, and professional experience including hiring and managing engineers engaged in the development of similar systems to the '785 Patent, I am familiar with the level and abilities of a POSITA at the time of the claimed invention. Additionally, I met at least these minimum qualifications to be a person having ordinary skill in the art at the time of the claimed invention. Further, although my qualifications may exceed those of the

UNIFIED PATENTS EXHIBIT 1003
Page 9 of 25

AA/SWA Ex. 1015, p.221 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

hypothetical POSITA defined above, my analysis and opinions regarding the '785 Patent have been rendered from the perspective of a POSITA at the time of the claimed invention.

B. Summary of My Opinions

31. I have reviewed the claims of the '785 Patent, the prior art cited in the Request for Ex Parte Reexamination, and the mapping of the prior art charted against the Challenged Claims 30 and 34 in Exhibit AA, and I agree with Requester that each of the Challenged Claims recites concepts that either are disclosed by, or are obvious variations of, the prior art grounds cited in the Request. The concept of a virtual private network system utilizing a registration system and a DNS server that returns multiple addresses was known years prior to the priority date of the '785 Patent.

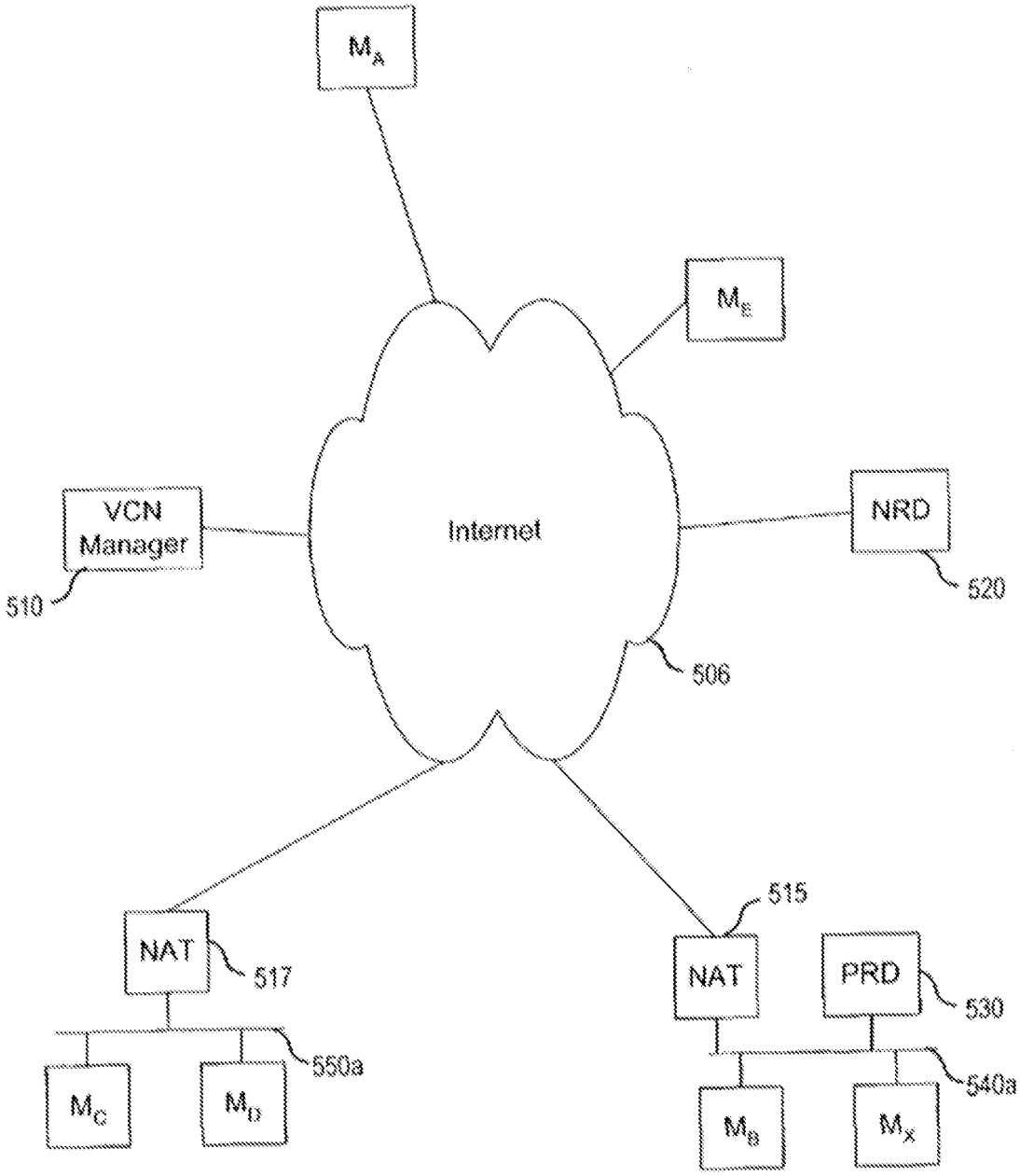
32. I note that the information I have provided is non-exhaustive, and there may be many additional materials that would reflect the common knowledge and skill of a POSITA by March 31, 2003 and that are relevant to the '785 Patent's claimed invention. Further, although there may be minor differences between cited disclosures of the prior art and the claims of the '785 Patent, in my opinion, a POSITA would not have appreciated some new synergy or unexpected results from the limitations given the disclosures of the prior art and the general knowledge of a POSITA.

C. Summary of the '785 Patent

33. The '785 Patent is generally directed to "[a] private virtual dynamic network … provided for computing devices coupled to public networks or private networks." Ex. 1001 ('785 Patent) at Abstract. The claims of the '785 Patent are directed to "a virtual network manager" or "a virtual network system" including "a network interface configured for data communication," "a register module configured to register devices in a virtual network," and "a DNS server configured to receive a DNS request … and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device." Ex. 1001 at 36:37-56 (claim 30). The '785 Patent discloses "a secure Virtual Community Network or 'VCN'" in which "all members of the VCN are accessible as if they were part of a physical local network" and "may all make direct connections to each other through communications within the virtual domain." Ex. 1001 at 8:66-9:41. The '785 Patent admits that "[a] hardware architecture for the machines, server or other devices used to implement the present invention should be well understood to one of average skill in the art" and "[s]uitable hardware includes one or more processors, a memory, a mass storage device, a portable storage device, a first network interface, a second network interface and I/O

devices, in communication with each other." Ex. 1001 at 9:42-48. An example of the system is shown in Figure 5A.

Fig. 5a



Ex. 1001 at Fig. 5A. The '785 Patent discloses that "[t]he choice of processor is not critical," "the

UNIFIED PATENTS EXHIBIT 1003
Page 11 of 25

AA/SWA Ex. 1015, p.223 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

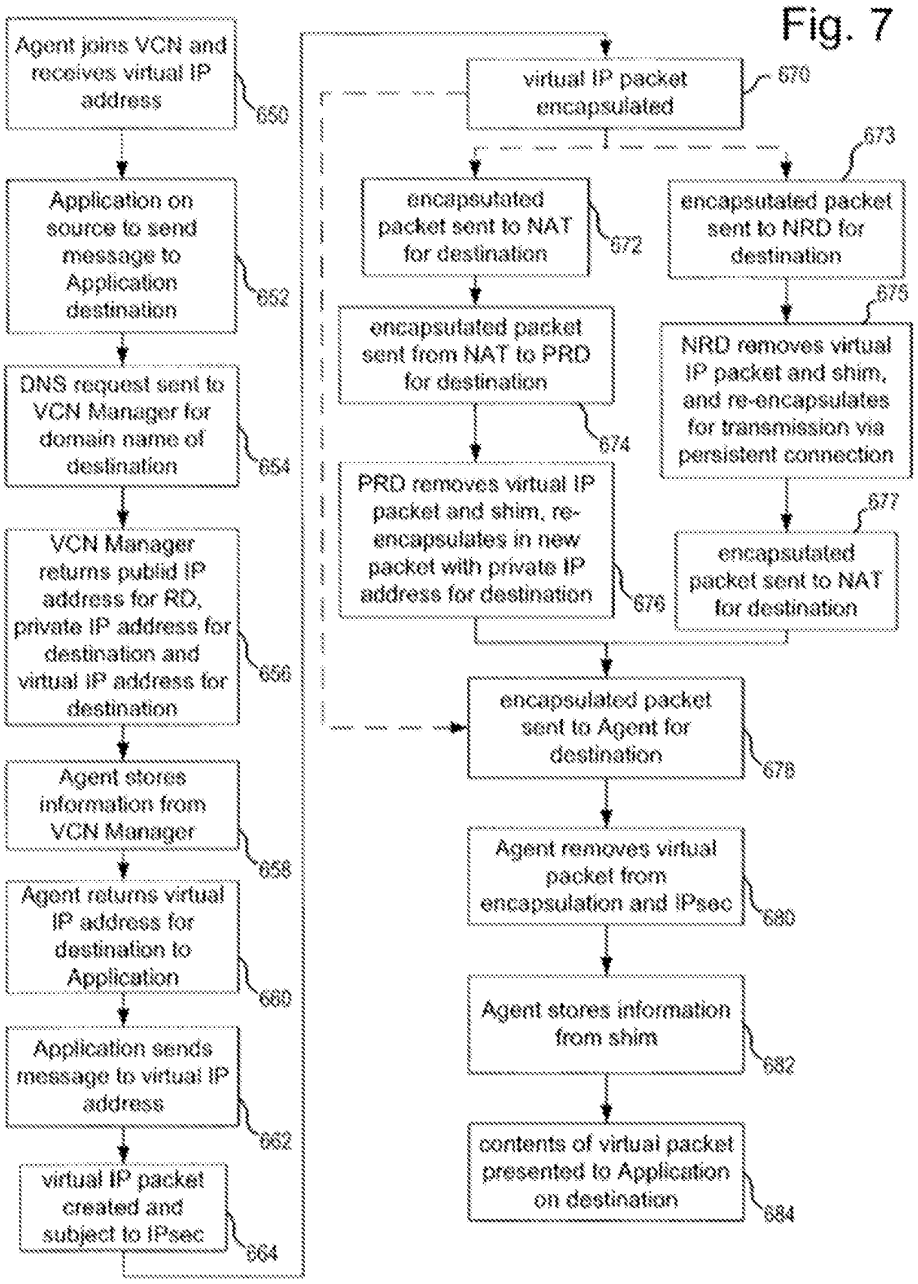
memory can be any conventional computer memory," and "[t]he network interface can include a network card for connecting to an Ethernet or other type of LAN." Ex. 1001 at 9:48-58.

34. The '785 Patent discloses that "various user machines M_n [are] coupled to the Internet 506, as well as other devices … which implement a virtual community in accordance with the present invention." Ex. 1001 at 10:17-20. "In general, an exemplary system for implementing a VCN in accordance with the invention comprises a VCN Manager 510, a Network Route Director 520 and/or Private Route Director 530, and a number of Member Agents 565." Ex. 1001 at 10:24-27. The '785 Patent notes that "[t]he VCN Manager 510 is a central server or server cluster providing management services, connection services and security services for the VCN." Ex. 1001 at 10:66-11:1.

35. The '785 Patent discloses that, "[i]n order to establish or participate in communication within the VCN, a device must register with and join the VCN, thereby becoming a member of the VCN" and, in order to do so, "[t]he Agent will send a message to VCN Manager 510 and receive a virtual IP address back," as shown in step 650 of Figure 7. Ex. 1001 at 14:10-15, Fig. 7.

UNIFIED PATENTS EXHIBIT 1003
Page 12 of 25

AA/SWA Ex. 1015, p.224 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786



36. When the new member device wants to send a message to another device in the VCN, it "will initiate a DNS request" and "[t]his DNS request is sent to the VCN Manager 510," as shown in step 654. Ex. 1001 at 14:32-34. In response to this request, "VCN Manager 510 returns the public address of the Route Director for the destination, the private address for the destination device and a virtual IP address for the destination device," as shown in Step 656. Ex.

1001 at 14:34-38. "Encapsulated UDP traffic is used by elements of the VCN once membership has been established and the elements are joined in the VCN for management and administrative communications." Ex. 1001 at 11:43-46.

D. Summary of the Prosecution History

37. Application 10/403,818 (the "'818 Application") was filed on March 31, 2003 with 109 proposed claims. In an office action on November 22, 2006, all claims were rejected as anticipated by US Patent Application Publication No. 2003/0041136 (Cheline). Ex. 1002 at 143-162. On March 22, 2007, the applicant filed a response along with a series of amendments. Ex. 1002 at 170-192. The applicant amended the earlier-filed claims by adding limitations specifying that the network traffic router "uses router data to route traffic between members of the virtual community" and that "a first member of the virtual community communicates with another member in the virtual community by querying the DNS server to determine a virtual network address and a private network address for the another member, and to determine a public address of the network traffic router." Ex. 1002 at 172-187. In its remarks, the applicant argued that "Cheline can hardly be considered to be a management device for a virtual community" and "the client 102(1) of Cheline does not communicate with the DNS server 120 to obtain a virtual network address and private network address of another client such as client 102(2) and to obtain a public network address of the service provider system 146, which is asserted by the Examiner to be a network traffic router as claimed.". Ex. 1002 at 190-191.

38. A final office action was issued on June 5, 2007 rejecting claims 93-100 and 102-109 for the same reasons as in the previous office action and claims 1-92 as obvious over Cheline in view of US Patent Application Publication No. 2004/0006708 (Mukherjee). Ex. 1002 at 202-213. The examiner found that Mukherjee teaches "at least one route director capable of communicating with users in the user set, the at least one route director routes traffic between the users," among other things. Ex. 1002 at 207-208. On November 5, 2007, the applicant responded by attempting to traverse the rejections. Ex. 1002 at 217-234. Specifically, the applicant argued the "Office Action does not address the amended claims." Ex. 1002 at 233.

39. The examiner then issued an Advisory Action Before Filing of an Appeal Brief on November 19, 2007. Ex. 1002 at 240-242. The applicant then filed a Request for Continued Examination (RCE) containing some minor amendments and arguments. Ex. 1002 at 243-267.

40. On February 13, 2008, the examiner issued another office action stating that the amendments were non-responsive. Ex. 1002 at 305-308. The applicant responded by amending the claims so as to rewrite them entirely. Ex. 1002 at 309-372. For example, claim 32 and 44 (which eventually were combined into issued claim 30) were amended as follows:

32. (currently amended) A ~~system~~ virtual network manager, comprising:

a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;

a register module configured to register devices in a virtual network, the register module further configured to:

receive a registration request from an agent associated with a device; and

distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address,

~~a management device for a virtual community, the management device including a network interface coupled to a public address realm and having a public address; and~~

~~a network traffic router which uses router data to route traffic between members of the virtual community, the router data including at least one association of a logical identifier with public routing information for a member.~~

44. (currently amended) The ~~system~~ virtual network manager of claim 32 further comprising a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device, ~~wherein each member receives a respective virtual network address when registering with the management device to join the virtual community, the management device includes a DNS server for the virtual community, a first member in the virtual community communicates with another member in the virtual community by querying the DNS server to determine a private network and the respective virtual network address for the another member, and to determine a public address of the network traffic router, and the first member communicates with the another member using an encapsulated packet having a source address which is the respective virtual network address of the first member and a destination address which is the respective virtual network address of the another member, by sending the encapsulated packet to the network traffic router in an encapsulating packet having a destination address which is the public address of the network traffic router, the private network address for the another member is included in the encapsulating packet and is used by the network traffic router to route the encapsulated packet to the another member.~~

Further, the applicant argued that "Cheline and/or Mukherjee do not teach a virtual network address, or a device being identified in a virtual network by a virtual network address, as recited in claim 32." Ex. 1002 at 347.

41. On February 4, 2009, another office action was issued rejecting all pending claims under 35 U.S.C. 101 and most claims as anticipated by or obvious over US Patent Application Publication No. 2008/0232295 (Kreiner). Ex. 1002 at 391-400. Claims 16 and 44

UNIFIED PATENTS EXHIBIT 1003
Page 16 of 25

AA/SWA Ex. 1015, p.228 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

were objected to as dependent upon a rejected base claim, but "would be allowable if rewritten in independent form." Ex. 1002 at 399. The examiner provided that "[t]he prior art does not teach he *[sic]* claimed relation between the elements claimed" as the reason for the indication of allowable subject matter. *Id.*

42. On May 29, 2009, the applicant responded to the office action by amending independent claims 1 and 32 to incorporate the subject matter of claims 16 and 44 and by amending the other independent claims in similar ways. Ex. 1002 at 437-465.

43. On November 29, 2009, the examiner issued another office action stating that certain of the amendments were non-responsive. Ex. 1002 at 489-492. The applicant responded on October 24, 2009 with mostly identical amendments, but including new arguments regarding claim 93. Ex. 1002 at 493-521. On February 5, 2010, the examiner issued a Notice of Non-Compliant Amendment (Ex. 1002 at 528-530) and the applicant responded on February 22, 2010 by correcting the amendments to only show claim 93 as currently amended. Ex. 1002 at 531-559. On June 1, 2010, the examiner issued another Notice of Non-Complaint Amendment related to the markings of claim 93 (Ex. 1002 at 579-581) and the applicant responded on June 7, 2010 by correcting the amendment to claim 93. Ex. 1002 at 582-610.

44. On September 1, 2010, the examiner issued another office action stating that claims 1-15, 17-24, 26-36, 41-43, and 93-109 were allowed and claims 53-66 and 68-92 were rejected as anticipated by US Patent No. 6631416 (Bendinelli). Ex. 1002 at 613-618. The examiner provided as reasons for allowance that "the prior art was not found to teach or suggest returning a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device in response to a DNS request in the context of claims 1, 32, and 93" and "[s]pecifically, **no examples were found in the prior art of record in which both a private address and a virtual address of a destination device would be returned.**" Ex. 1002 at 616-617. The applicant responded on October 21. 2010 by amending claims 53-55, 64, and 80 to include a similar DNS request and response element. Ex. 1002 at 658-683.

45. On November 5, 2010, the examiner issued another office action rejecting claims 1-15, 17-24, 26-36, 41-43, and 80-92 as invalid under 35 U.S.C. 101, but otherwise containing allowable subject matter. Ex. 1002 at 687-691. The applicant responded on December 2, 2010 by amending those claims "to clarify that the recited virtual network manager and/or route director

are implemented with a memory and a processor of a computing device." Ex. 1002 at 723-750. For example, claim 32 was amended as follows:

> **32. (currently amended)** A virtual network manager, comprising:
>
> a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;
>
> a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to:
>
> receive a registration request from an agent associated with a device;
>
> distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and
>
> a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.

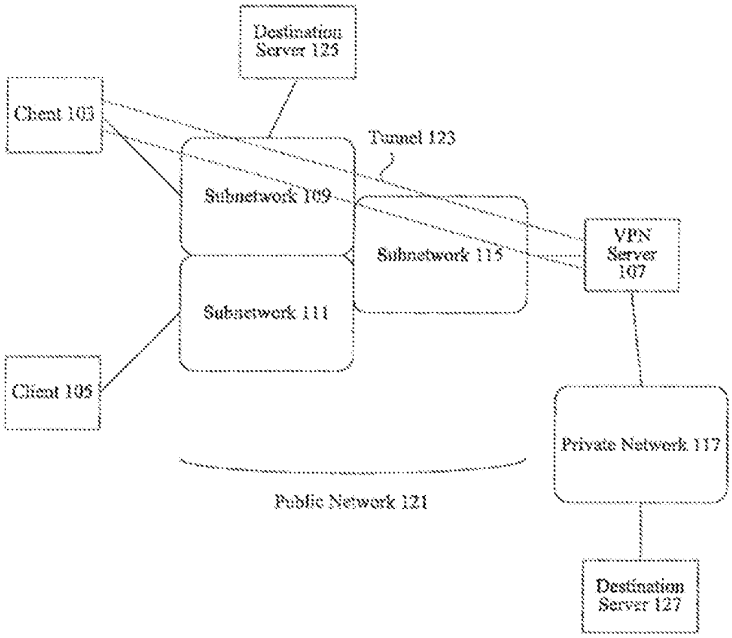
46. The examiner issued a Notice of Allowance on January 14, 2011. Ex. 1002 at 760-766.

E. Ground 1: *Leung* in view of *Forslöw* and *Mehta*

1. Overview of Leung

47. *Leung* (**Ex. 1005,** U.S. Patent No. 7,036,143) discloses a virtual private network system in which "the VPN client can establish sessions with a variety of destination nodes including destination nodes on a private or enterprise network associated with the VPN server." Ex. 1005 (*Leung*), Abstract. This system is shown in Figure 1.

Figure 1



Id. at Fig. 1.

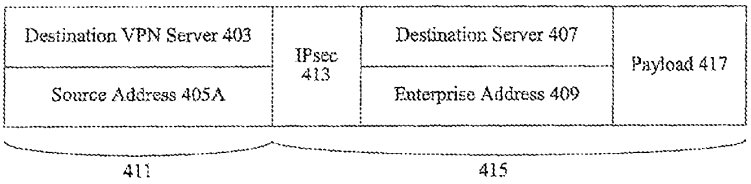
48. *Leung* discloses that "the public network 121 is connected to private network 117 through a VPN server 107." *Id.* at 4:57-64. *Leung* discloses that "the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general purpose computing device." *Id.* at 11:12-17. *Leung* discloses that "client 103 may acquire a subnetwork address from the Internet service provider associated with subnetwork 109." *Id.* at 4:66-5:11. A POSITA would have understood that the subnetwork address obtained from the Internet service provider disclosed in *Leung* is based on the domain name of the public network because, as explained in *Leung*, "[u]sing the subnetwork address, client 103 can access a destination server 125 in a public network 121. However, client 103 can not access a private network destination server 127 until it is granted access by VPN server 107." *Id.* at 5:10-13. Thus, a POSITA would have understood that the client must know the domain name of the public network 121 in order to access the VPN server 107. For that reason, it would have been obvious for *Leung*'s virtual network to have been defined by a domain name.

49. *Leung* further discloses that "[t]o acquire access to destination server 127 in a

private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107," including "information such as its subnetwork address, its user name, and its password." *Id.* at 5:11-18. A POSITA would have understood that *Leung*'s VPN clients would send registration requests via an associated agent. The '785 Patent describes "communication agent[s] installed on a device" that can include "software or hardware" and "may comprise a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address." Ex. 1001 at 7:1-8. Similarly, a POSITA would have understood *Leung*'s VPN clients to include software to allow traffic to be routed to members of the virtual community. Such virtual network adapter software would have been required in *Leung* for such a client device to send an access request to the VPN server because the very purpose of a VPN is to allow secure communication among its members and to deny communication to non-members.

50. In response, the VPN server provides the client with an "enterprise address," which "is the address that the VPN client users to communicate with other nodes such as nodes in the company private network." *Id.* at 4:5-10. *Leung* explains that "other nodes including nodes in the company private network will see the VPN client as having the enterprise address, and will therefore communicate with the VPN client via the enterprise address." *Id.* at 4:12-25. Upon receiving the enterprise address, the client can communicate via a VPN tunnel via encapsulated packets. For example, "the encapsulated portion 415 preferably contains the enterprise address 409 allocated by the VPN server to the VPN client during the creation of the VPN tunnel, which may be used to authenticate the sender," as shown in Figure 4A. *Id.* at 6:53-67.

Figure 4A



Id. at Fig. 4A.

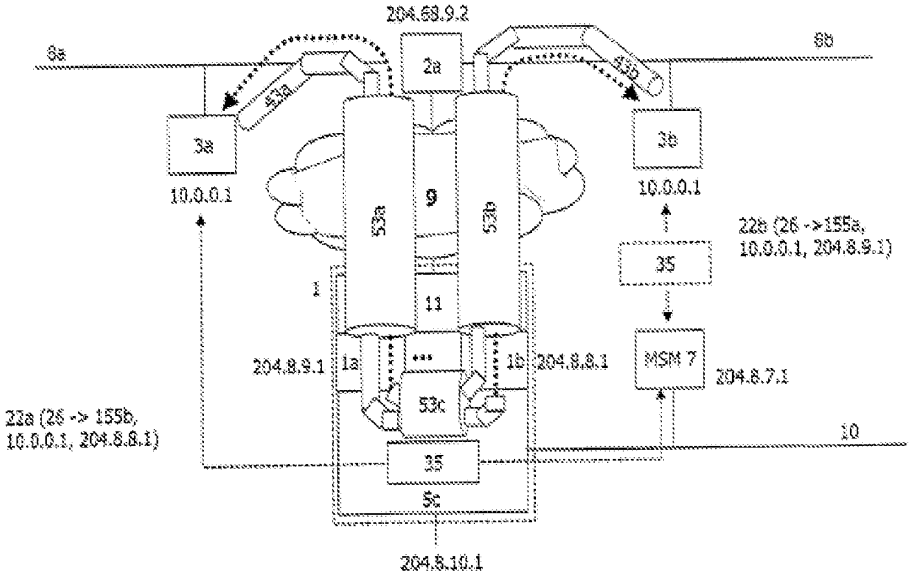
2. Overview of Forslöw

51. *Forslöw* (**Ex. 1006,** U.S. Patent No. 7,155,518) discloses "a network-based

AA/SWA Ex. 1015, p.232 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

mobile workgroup system showing a selected set of users from two or more mobile virtual private networks to form an extranet workgroup in a secure manner." Ex. 1006 (*Forslöw*), Abstract. *Forslöw* discloses that its "system also entails a mobile service manager that has a public IP address and a set of mobile nodes that all have a UFQDN (user fully qualified domain name) within the overall mobile workgroup system." *Id.*, Abstract. A UFQDN has the form of a FQDN (one that resolves to a unique IP address) that is preceded by a username and the "@" character. Email addresses typically have the form of a UFQDN, e.g., shamos@cs.cmu.edu, my email address. The FQDN is "cs.cmu.edu" and the username is "shamos," forming the UFQDN shamos@cs.cmu.edu. The UFQDN allows access to a particular node within a workgroup. This system is shown in Figure 2.

Fig. 2



Id. at Fig. 2. "FIG. 2 shows the tunnel structure that is established in order to allow two mobile nodes 3a and 3b to be part of the same extranet workgroup in a secure manner." *Id.* at 9:62-10:6.

52. *Forslöw* discloses that backbone virtual home agent 5c "act[s] as the common gateway towards the Internet 6 for all virtual home agents 1a and 1b" and "also hosts a management network 10 to which a mobile service manager 7 for the mobile workgroup system is attached." *Id.* at 9:30-43. "The mobile nodes 3a and 3b that are belonging to an extranet

workgroup retrieve a list of workgroup members 26 by doing HTTPS requests 22a and 22b to the mobile service manager 7," which functions as a DNS server. *Id.* at 10:7-20. These requests are sent to the mobile service manager 7 and it returns "a triplet including the user fully qualified domain name 155 b/155 a, the mobile node 3 private IP address 156 a/b (10.0.0.1) and the virtual home agent's 1 a/1 b public IP address 157 a/b (204.8.9.1 and 204.8.8.1 respectively)." *Id.*; *see also id.* at 11:9-17. 11:18-28. *Forslöw* further discloses that "[t]he center module of a virtual home agent 1a/b is the virtual router 5 a/b," which "is making nexthop decisions for datagrams passing through the virtual home agent 1 a/b." *Id.* at 12:14-21.

3. Overview of Mehta

53. *Mehta* (**Ex. 1007**, U.S. Patent Publication No. 2003/0028671) discloses a system "for initiating communication with a device on a private network from a device on a public network to achieve virtual end-to-end connectivity." Ex. 1007 (*Mehta*) at [0002]. Figure 2 provides an example of *Mehta*'s system.

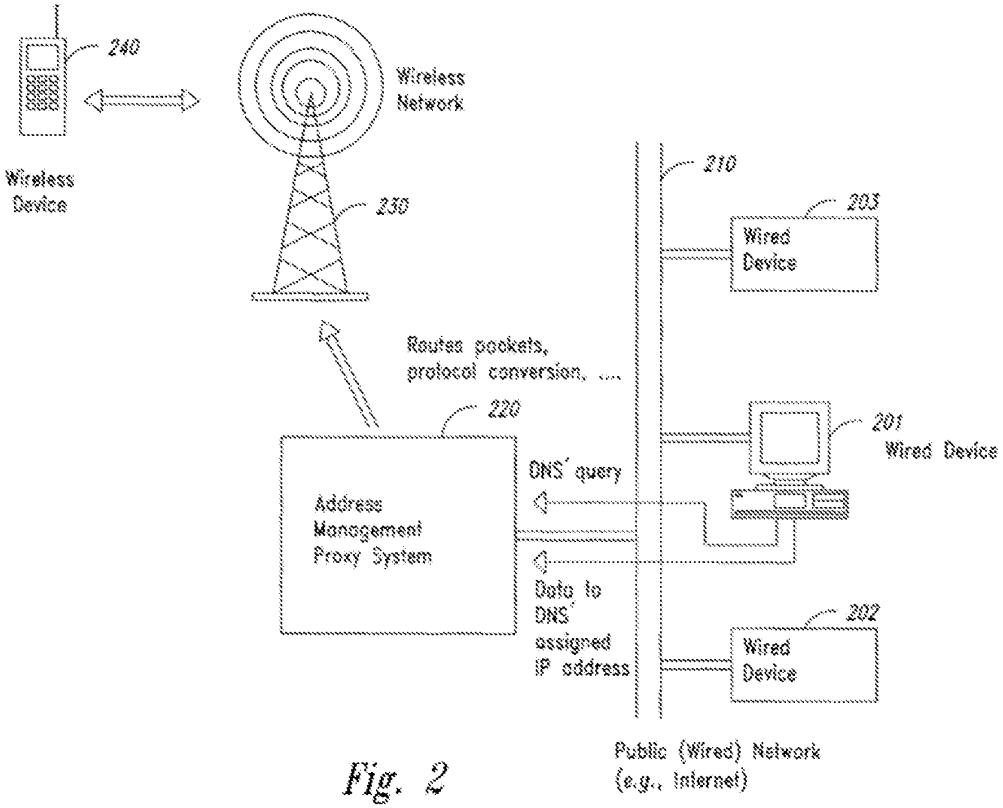


Fig. 2

Ex. 1007 at Fig. 2.

54. *Mehta* discloses example embodiments that provide "an Address Management

Proxy System ("AMPS"), which enables devices and systems connected to a public internetwork, such as the Internet, to initiate communication with and send data to wireless devices connected to a private wireless network." Ex. 1007 at [0011]. *Mehta* discloses that "the AMPS comprises one or more modified DNS/API servers, one or more Address Proxy/Routers, an Address Management Data Server, one or more Address Management Data Repositories, and optionally a load balancer." *Id.* at [0012]. "The AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device, and returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device." *Id. Mehta* discloses that this "temporary public address is, for example, an address associated with one of the Address Proxy/Routers, which are connected to the external public network and have access to the private addresses on the private wireless network" and that it "is then usable by the device on the externsal public network to send data to the wireless device." *Id.*

55. More specifically, "the wired device 201 performs a query (for example, a modified DNS query) to locate a routable public address that corresponds to wireless device 240" and then "[t]he Address Management Proxy System 220 receives the query and determines and assigns a public (routable) address from a pool of addresses, which address can be used as a destination address for data packets targeted to wireless device 240." *Id.* at [0031]. At that point, "[d]ata is sent to a particular Address Proxy/Router because the public (routable) address of that Address Proxy /Router was returned to the requesting/ source device in response to a query of the DNS'/API server of the AMPS." *Id.* at [0058].

4. Motivation to Combine *Leung* with *Forslöw* and *Mehta*

56. In my opinion, a POSITA would have found it obvious to incorporate *Forslöw*'s and *Mehta*'s teachings related to a communication across virtual networks into *Leung*'s virtual private network system. *Leung* discloses a VPN system in which client devices gain access to the VPN in order to send data to devices within the VPN. See, e.g., Ex. 1005 at 5:8-18. *Forslöw* discloses a similar VPN, but specifically goes into detail in describing the way in which the DNS server (which it calls a mobile service manager) facilitates communication over the VPN system. See, e.g., Ex. 1006 at 9:62-10:20. A POSITA would have been motivated to make such a combination because implementation of *Forslöw*'s VPN tunnelling system would have allowed data messaging to be sent in a more efficient and secure manner.

57. Additionally, *Forslöw*'s VPN system provides for a virtual route director to assist in data mapping. See, e.g., Ex. 1006 at 9:19-29. *Mehta* discloses a similar virtual networking

system that operates with a DNS server and a route director, but it goes into more details about the operation of the route director, and thus provides for such DNS servers to provide private to network address associated with a network address proxy machine. See, e.g., Ex. 1007 at [0012], [0031]-[0032]. A POSITA would have been motivated to make this combination because implantation of *Mehta*'s utilization of the DNS server would have aided in the security of the VPN system created by the combination of *Leung* and *Forslöw*.

58. Furthermore, a POSITA would have been motivated to combine *Leung, Forslöw*, and *Mehta* because the combination merely uses a known technique to improve similar devices in the same way. See *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 401 (2007). For instance, the combination would have merely required the use of a known technique, specifically the utilization of routing via addresses provided by a DNS server to similar VPN systems in the same way. For instance, *see, e.g.*, Ex. 1008 (Kong) at 2:15-42 ("the direct connection part comprises an address acquisition part for acquiring a public IP address of the second private network from a domain name management server based on a domain name of the second network device received from the first network device, and for acquiring a private IP address of the second network device based on the received domain name."), 5:17-6:5 ("The address acquisition part 242 acquires a public IP address from the Domain Name Server 120."); Ex. 1009 (Volz) at 5:13-26, 11:31-64 ("an outside node that wants to initiate a new connection to a particular inside node prepares a user-resource identifier query"), 19:47-20:15 ("node B application server sends a DNS-query … [and t]he resource manager 40 then sends a reply including the public gateway address allocated to node A").

59. A POSITA would have had a reasonable expectation of success in modifying *Leung*'s VPN system, which allows for registration and data transmission by client devices, to perform this data transmission via use of a DNS server and route director, as taught by *Forslöw* and *Mehta*, because doing so would merely have implemented a well-known technique in the VPN system of *Leung*, as shown in Exhibit AA.

60. In addition, a POSITA would have been motivated to modify the virtual network of *Leung* to incorporate the property of the virtual network of *Forslöw* that it is defined by a user fully qualified domain name (UFQDM). This is true because a POSITA would have understood that *Leung*'s virtual network requires knowledge of such a domain name to access the VPN server, as I explained above in paragraph 49. Thus, a POSITA would have looked to a system, such as *Forslöw*, which explicitly explains that such a virtual network would have been defined by a

particular type of domain name, i.e., a user fully qualified domain name. *See* Paragraph 51, above.

61. *Leung* combined with *Forslöw* and *Mehta* teaches every limitation of every Challenged Claim. As mentioned, a POSITA would have been motivated to combine, and would have had a reasonable expectation of success in combining, *Forslöw's* and *Mehta's* teachings related to the use of a DNS server in a virtual network system with Leung's teaching related to a VPN system. Thus, *Leung*, in combination with *Forslöw* and *Mehta*, renders the Challenged Claims obvious.

IV. CONCLUSION

62. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: 5/22/2024

By: 

Michael I. Shamos

UNIFIED PATENTS EXHIBIT 1003
Page 25 of 25

AA/SWA Ex. 1015, p.237 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of Alkhatib et al.	§	REQUEST FOR *Ex Parte* REEXAMINATION
U.S. Patent No.: 7,949,785	§	
	§	Attorney Docket No.: IVI785
Issue Date: May, 24, 2011	§	
	§	Customer No.: 165774
Filing Date: March, 31, 2003	§	
	§	
Title: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM	§	
	§	
	§	
	§	

CERTIFICATE OF SERVICE

The undersigned certifies that copies of the following,

(1) *Request for Ex Parte Reexamination* Transmittal Form for U.S. Patent No. 7,949,785;

(2) *Request for Ex Parte Reexamination* of U.S. Patent No.7,949,785;

(3) Information Disclosure Statement by Requester; and

(4) Exhibits 1001 through 1010 and Exhibit AA, which includes a copy of the patent to be reexamined as Exhibit 1001;

(5) Certificate of Service.

in their entirety were served on:

MCANDREWS HELD & MALLOY, LTD

500 WEST MADISON STREET

SUITE 3400

CHICAGO, IL 23446

the attorney of record for the assignee of U.S. Patent No. 7,949,785, in accordance with 37 C.F.R. § 1.510(b)(5), on May 22, 2024, by the U.S. Postal Service Priority Express mail.

Dated: May 22, 2024

/Jordan M. Rossen/

Jordan M. Rossen
Unified Patents, LLC
jordan@unifiedpatents.com
Attorney for Third Party Requester
Registration No.: 74,064

EXHIBIT 1010

Infringement Claim Chart from *Intellectual Ventures I LLC et al v. Comerica Inc.*, Case No. 2:23-cv-00524, Dkt. 1, Ex. 9 (E.D. Tex. Nov. 15, 2023)

Exhibit 9

Exhibit 9 to Complaint
Intellectual Ventures I LLC and Intellectual Ventures II LLC

Example Comerica Count IV Systems and Services
U.S. Patent No. 7,949,785 ("the '785 Patent")

The Accused Systems and Services include, without limitation, Comerica's systems that utilize Apache Spark ("Spark"); all past, current and future systems and services that operate in the same or substantially similar manner as the specifically identified systems and services; and all past, current and future Comerica's systems and services that have the same or substantially similar features as the specifically identified systems and services ("Example Comerica Count IV Systems and Services").

UNIFIED PATENTS EXHIBIT 1010
Page 3 of 19

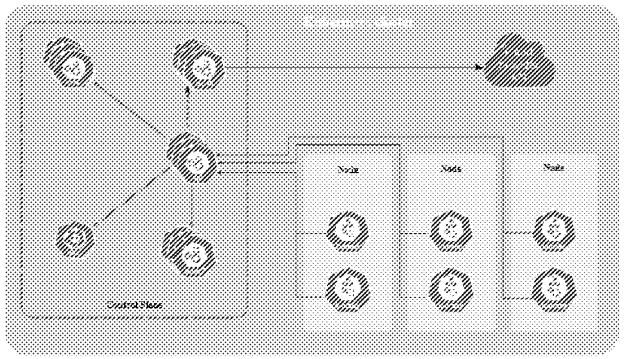
AA/SWA Ex. 1015, p.243 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

U.S. Patent No. 7,949,785	
Example Claim 30	**Accused Instrumentalities: Example Comerica Count IV Systems and Services**
30. A virtual network manager, comprising:	Upon information and belief, the Comerica's systems include "a virtual network manager." The virtual network manager is the Kubernetes functionality related to DNS for Services and Pods. **DNS for Services and Pods** Kubernetes creates DNS records for Services and Pods. You can contact Services with consistent DNS names instead of IP addresses. Kubernetes publishes information about Pods and Services which is used to program DNS. Kubelet configures Pods' DNS so that running containers can lookup Services by name rather than IP. Services defined in the cluster are assigned DNS names. By default, a client Pod's DNS search list includes the Pod's own namespace and the cluster's default domain. *See* https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/#pod-s-dns-config (last accessed on November 11, 2023). A Service in Kubernetes is an abstraction which defines a logical set of Pods and a policy by which to access them. Services enable a loose coupling between dependent Pods. A Service is defined using YAML or JSON, like all Kubernetes object manifests. The set of Pods targeted by a Service is usually determined by a *label selector* (see below for why you might want a Service without including a `selector` in the spec). *See* https://kubernetes.io/docs/tutorials/kubernetes-basics/expose/expose-intro/ (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 4 of 19
AA/SWA Ex. 1015, p.244 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	Kubernetes assigns this Service an IP address (the *cluster IP*), that is used by the virtual IP address mechanism. For more details on that mechanism, read Virtual IPs and Service Proxies. *See* https://kubernetes.io/docs/concepts/services-networking/service/ (last accessed on November 11, 2023). **Virtual IPs and Service Proxies** Every node in a Kubernetes cluster runs a kube-proxy (unless you have deployed your own alternative component in place of `kube-proxy`). The `kube-proxy` component is responsible for implementing a *virtual IP* mechanism for Services of `type` other than `ExternalName`. *See* https://kubernetes.io/docs/reference/networking/virtual-ips/ (last accessed on November 11, 2023). Comerica's systems include Kubernetes functionality. *See, e.g.*, https://careers.comerica.com/job/19419241/principal-engineer-cloud-automation-governance-and-engineering-cage-dallas-or-detroit-metro-auburn-hills-mi/ (last accessed on November 13, 2023).
a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;	Upon information and belief, the Comerica's systems utilize Kubernetes and include "a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address." For example, Kubernetes DNS for Services and PODS is implemented in part through a network interface called kube-proxy, which maintains network rules that allow communication to pods from network sessions. Kube-proxy communications can relate to network sessions inside or outside of the cluster (the virtual network) in which the services are defined. The services defined in the cluster are assigned DNS names having an associated public network address.

UNIFIED PATENTS EXHIBIT 1010
Page 5 of 19
AA/SWA Ex. 1015, p.245 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	Kubernetes Components  kube-proxy kube-proxy is a network proxy that runs on each node in your cluster, implementing part of the Kubernetes Service concept. kube-proxy maintains network rules on nodes. These network rules allow network communication to your Pods from network sessions inside or outside of your cluster. *See* https://kubernetes.io/docs/concepts/overview/components/ (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 6 of 19
AA/SWA Ex. 1015, p.246 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	DNS A cluster-aware DNS server, such as CoreDNS, watches the Kubernetes API for new Services and creates a set of DNS records for each one. If DNS has been enabled throughout your cluster then all Pods should automatically be able to resolve Services by their DNS name. External IPs If there are external IPs that route to one or more cluster nodes, Kubernetes Services can be exposed on those externalIPs. When network traffic arrives into the cluster, with the external IP (as destination IP) and the port matching that Service, rules and routes that Kubernetes has configured ensure that the traffic is routed to one of the endpoints for that Service. *See* https://kubernetes.io/docs/concepts/services-networking/service/ (last accessed on November 11, 2023). **DNS for Services and Pods** Kubernetes creates DNS records for Services and Pods. You can contact Services with consistent DNS names instead of IP addresses. Services defined in the cluster are assigned DNS names. By default, a client Pod's DNS search list includes the Pod's own namespace and the cluster's default domain. *See* https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/#pod-s-dns-config (last accessed on November 11, 2023).

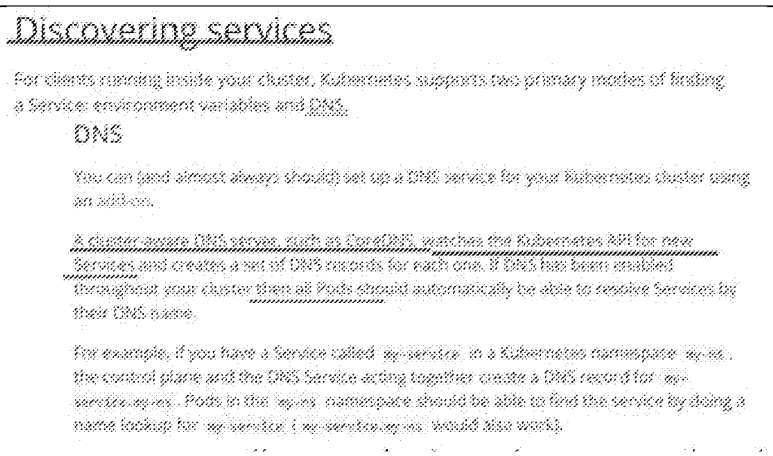
UNIFIED PATENTS EXHIBIT 1010
Page 7 of 19
AA/SWA Ex. 1015, p.247 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

a memory and a processor to implement a register module configured to register devices in a virtual network	Upon information and belief, the Comerica's systems utilize Kubernetes and includes "a memory and a processor to implement a register module configured to register devices in a virtual network." A service runs on a set of pods (devices). The Kubernetes DNS Service module (register module) watches the Kubernetes API for incoming new services and creates a set of DNS records for each of the pods associated with the service (register devices). Kubernetes runs your workload by placing containers into Pods to run on Nodes. A node may be a virtual or physical machine, depending on the cluster. Each node is managed by the control plane and contains the services necessary to run Pods. *See* https://kubernetes.io/docs/concepts/architecture/nodes (last accessed on November 11, 2023). Initializing your control-plane node The control-plane node is the machine where the control plane components run, including etcd (the cluster database) and the API Server (which the kubectl command line tool communicates with). *See* https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/create-cluster-kubeadm/ (last accessed on November 11, 2023). DNS ∞ You can (and almost always should) set up a DNS service for your Kubernetes cluster using an add-on. A cluster-aware DNS server, such as CoreDNS, watches the Kubernetes API for new Services and creates a set of DNS records for each one. If DNS has been enabled throughout your cluster then all Pods should automatically be able to resolve Services by their DNS name. For example, if you have a Service called my-service in a Kubernetes namespace my-ns, the control plane and the DNS Service acting together create a DNS record for my-service.my-ns. Pods in the my-ns namespace should be able to find the service by doing a name lookup for my-service (my-service.my-ns would also work). *See* https://kubernetes.io/docs/concepts/services-networking/service (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 8 of 19
AA/SWA Ex. 1015, p.248 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	Services in Kubernetes The Service API, part of Kubernetes, is an abstraction to help you expose groups of Pods over a network. Each Service object defines a logical set of endpoints (usually these endpoints are Pods) along with a policy about how to make those pods accessible. For example, consider a stateless image-processing backend which is running with 3 replicas. Those replicas are fungible—frontends do not care which backend they use. While the actual Pods that compose the backend set may change, the frontend clients should not need to be aware of that, nor should they need to keep track of the set of backends themselves. The Service abstraction enables this decoupling. The set of Pods targeted by a Service is usually determined by a selector that you define. To learn about other ways to define Service endpoints, see Services without selectors. *See* https://kubernetes.io/docs/reference/kubectl/cheatsheet/ (last accessed on November 11, 2023).
the register module further configured to: receive a registration request from an agent associated with a device;	Upon information and belief, the Comerica's systems include "the register module further configured to receive a registration request rom an agent associated with a device." A service runs on a set of pods. The Kubernetes DNS Service module (register module) watches the Kubernetes API for incoming new services (registration requests) being made via tools like kubctl (agent associated with a device). *See* https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/create-cluster-kubeadm/ (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 9 of 19
AA/SWA Ex. 1015, p.249 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786



Discovering services

For clients running inside your cluster, Kubernetes supports two primary modes of finding a Service: environment variables and DNS.

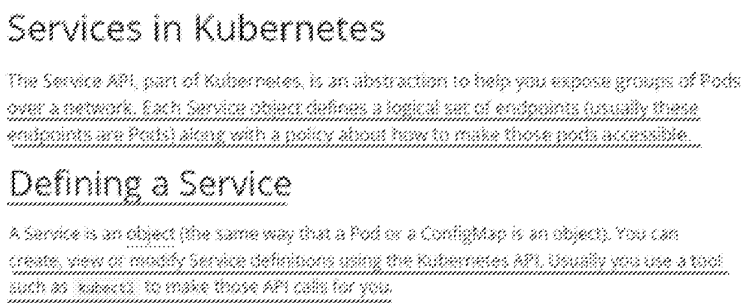
DNS

You can (and almost always should) set up a DNS service for your Kubernetes cluster using an add-on.

A cluster-aware DNS server, such as CoreDNS, watches the Kubernetes API for new Services and creates a set of DNS records for each one. If DNS has been enabled throughout your cluster then all Pods should automatically be able to resolve Services by their DNS name.

For example, if you have a Service called `my-service` in a Kubernetes namespace `my-ns`, the control plane and the DNS Service acting together create a DNS record for `my-service.my-ns`. Pods in the `my-ns` namespace should be able to find the service by doing a name lookup for `my-service` (`my-service.my-ns` would also work).

See https://kubernetes.io/docs/concepts/services-networking/service (last accessed on November 11, 2023).



Services in Kubernetes

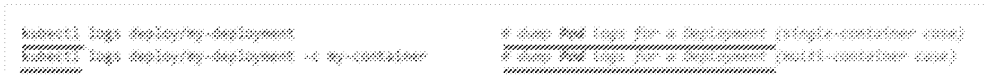
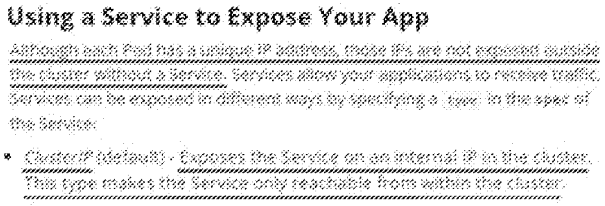
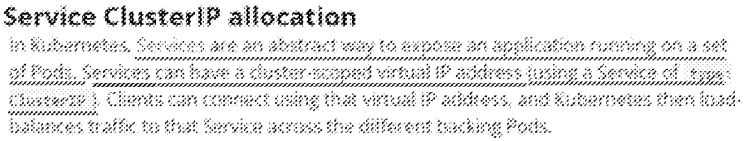
The Service API, part of Kubernetes, is an abstraction to help you expose groups of Pods over a network. Each Service object defines a logical set of endpoints (usually these endpoints are Pods) along with a policy about how to make those pods accessible.

Defining a Service

A Service is an object (the same way that a Pod or a ConfigMap is an object). You can create, view or modify Service definitions using the Kubernetes API. Usually you use a tool such as `kubectl` to make those API calls for you.

See https://kubernetes.io/docs/concepts/services-networking/service (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 10 of 19
AA/SWA Ex. 1015, p.250 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	 *See* https://kubernetes.io/docs/reference/kubectl/cheatsheet/ (last accessed on November 11, 2023).
distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and	Upon information and belief, the Comerica's systems include a register module further configured to "distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address." A service runs on a set of pods. A new service is assigned to a cluster IP ("virtual network address"). As part of configuration, the Kubernetes DNS Service module distributes the network address to at least one pod (deice) on which the service runs.  *See* https://kubernetes.io/docs/tutorials/kubernetes-basics/expose/expose-intro/ (last accessed on November 11, 2023).  *See* https://kubernetes.io/docs/concepts/services-networking/cluster-ip-allocation/ (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 11 of 19
AA/SWA Ex. 1015, p.251 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

VIP

a virtual IP address, such as the one assigned to every Service in Kubernetes

See https://kubernetes.io/docs/tutorials/services/source-ip/ (last accessed on November 11, 2023).

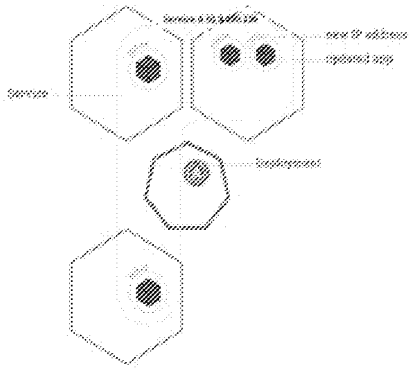
DNS

You can (and almost always should) set up a DNS service for your Kubernetes cluster using an add-on.

A cluster-aware DNS server, such as CoreDNS, watches the Kubernetes API for new Services and creates a set of DNS records for each one. If DNS has been enabled throughout your cluster then all Pods should automatically be able to resolve Services by their DNS name.

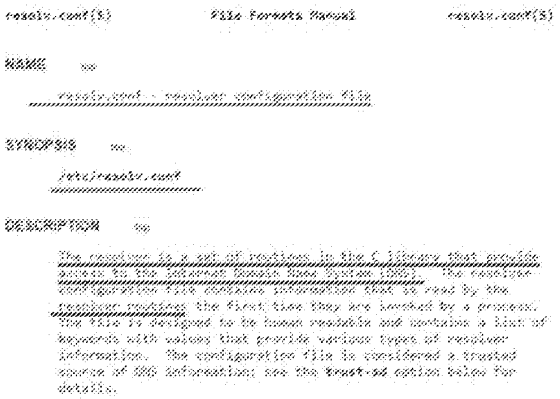
For example, if you have a Service called `my-service` in a Kubernetes namespace `my-ns`, the control plane and the DNS Service acting together create a DNS record for `my-service.my-ns`. Pods in the `my-ns` namespace should be able to find the service by doing a name lookup for `my-service` (`my-service.my-ns` would also work).

See https://kubernetes.io/docs/concepts/services-networking/service (last accessed on November 11, 2023).



UNIFIED PATENTS EXHIBIT 1010
Page 12 of 19

AA/SWA Ex. 1015, p.252 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	See https://kubernetes.io/docs/tutorials/kubernetes-basics/update/update-intro/ (last accessed on November 11, 2023).
a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network and return a network address associated with a network route director,	Upon information and belief, the Comerica's systems include "a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network." A client/ frontend pod ("a first device") sends a DNS query ("DNS Request") using Kubernetes DNS query functionality, such as CoreDNS or kube-dns, which, includes resolver routines associated with the requesting pod. The DNS server (cluster DNS server (e.g. CoreDNS or kube dns)) is configured to return an IP address of cluster DNS server, which is referenced/returned by the process of the kubelet accessing resolv.conf.  *See* https://man7.org/linux/man-pages/man5/resolv.conf.5.html (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 13 of 19
AA/SWA Ex. 1015, p.253 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Using CoreDNS for Service Discovery

About CoreDNS

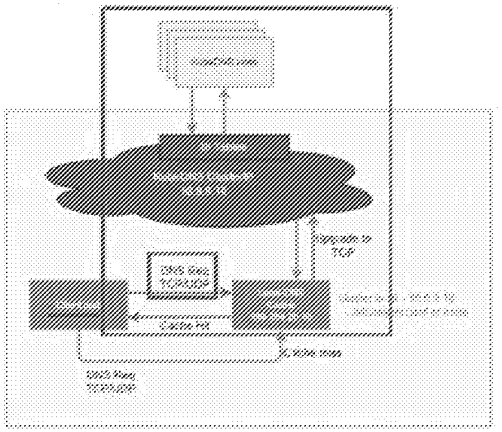
CoreDNS is a flexible, extensible DNS server that can serve as the Kubernetes cluster DNS. Like Kubernetes, the CoreDNS project is hosted by the CNCF.

You can use CoreDNS instead of kube-dns in your cluster by replacing kube-dns in an existing deployment, or by using tools like kubeadm that will deploy and upgrade the cluster for you.

See https://kubernetes.io/docs/tasks/administer-cluster/coredns/ (last accessed on November 11, 2023).

Introduction

NodeLocal DNSCache improves Cluster DNS performance by running a DNS caching agent on cluster nodes as a DaemonSet. In today's architecture, Pods in 'ClusterFirst' DNS mode reach out to a kube-dns `serviceIP` for DNS queries. This is translated to a kube-dns/CoreDNS endpoint via iptables rules added by kube-proxy. With this new architecture, Pods will reach out to the DNS caching agent running on the same node, thereby avoiding iptables DNAT rules and connection tracking. The local caching agent will query kube-dns service for cache misses of cluster hostnames ("cluster.local" suffix by default).



UNIFIED PATENTS EXHIBIT 1010
Page 14 of 19
AA/SWA Ex. 1015, p.254 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	See https://kubernetes.io/docs/tasks/administer-cluster/nodelocaldns/ (last accessed on November 11, 2023). **Pod to** When a pod sends an API request to a service within the same Kubernetes cluster, it must first resolve the IP address of the service. To do this, the pod performs a DNS lookup using the DNS server specified in its /etc/resolv.conf configuration file. This file, which is provisioned by the Kubelet, defines the settings for DNS lookups in the pod. It contains a reference to the cluster DNS server. By default, this configuration file looks something like this: search namespace.svc.cluster.local svc.cluster.local cluster.local nameserver 10.32.0.10 options ndots:5

UNIFIED PATENTS EXHIBIT 1010
Page 15 of 19

AA/SWA Ex. 1015, p.255 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

When a pod performs a DNS lookup, the query is first sent to the local DNS resolver in the pod. This resolver uses the /etc/resolv.conf configuration file. In this file, the nameserver is set up as the default resolver. DNS resolves which nameserver to use.

If the cache does not contain the IP address for the requested hostname, the query is forwarded to the cluster DNS server (kube-dns).

This DNS server determines the IP address by consulting the Kubernetes service registry. This registry contains a mapping of service names to their corresponding IP addresses. This allows the cluster DNS server to return the correct IP address to the requesting pod.

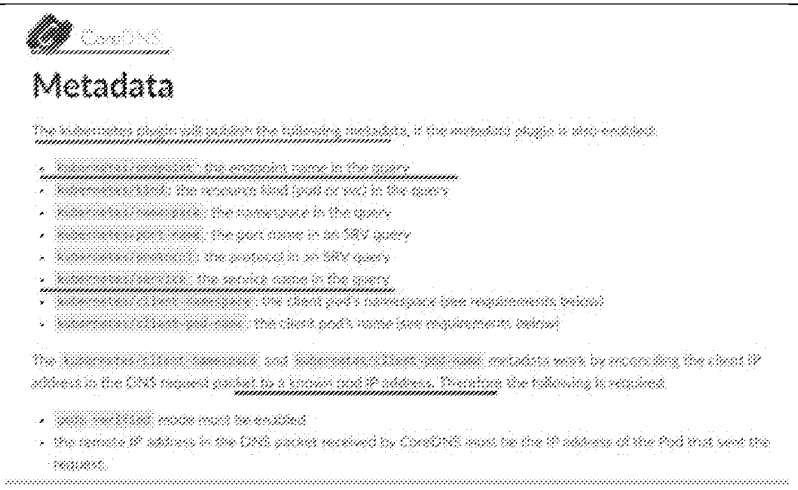
Any domains that are queried but are not in the Kubernetes service registry are forwarded to an upstream DNS server.

We will go through each of these components in more detail step by step.

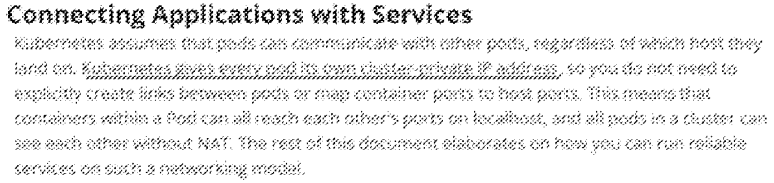
See https://medium.com/@selfeddinerajbi/connecting-the-dots-understanding-how-pods-talk-in-kubernetes-networks-992fa69ffbeb (last accessed on November 14, 2023).

a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.	Upon information and belief, the Comerica's systems include "a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device." The private network address associated with a second device is a unique private IP address assigned to a backend pod. The virtual network address associated with the second device is the Cluster IP or Virtual IP assigned to a set of pods.  CoreDNS kubernetes Description This plugin implements the Kubernetes DNS-Based Service Discovery Specification. CoreDNS running the kubernetes plugin can be used as a replacement for kube-dns in a kubernetes cluster. See the deployment repository for details on how to deploy CoreDNS in Kubernetes.

UNIFIED PATENTS EXHIBIT 1010
Page 17 of 19
AA/SWA Ex. 1015, p.257 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786



See https://coredns.io/plugins/kubernetes// (last accessed on November 11, 2023).



See https://kubernetes.io/docs/tutorials/services/connect-applications-service/ (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 18 of 19
AA/SWA Ex. 1015, p.258 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

	Using a Service to Expose Your App Although each Pod has a unique IP address, those IPs are not exposed outside the cluster without a Service. Services allow your applications to receive traffic. Services can be exposed in different ways by specifying a `type` in the spec of the Service: • *ClusterIP* (default) - Exposes the Service on an internal IP in the cluster. This type makes the Service only reachable from within the cluster. *See* https://kubernetes.io/docs/tutorials/kubernetes-basics/expose/expose-intro/ (last accessed on November 11, 2023). **Service ClusterIP allocation** In Kubernetes, Services are an abstract way to expose an application running on a set of Pods. Services can have a cluster-scoped virtual IP address (using a Service of `type: ClusterIP`). Clients can connect using that virtual IP address, and Kubernetes then load-balances traffic to that Service across the different backing Pods. *See* https://kubernetes.io/docs/concepts/services-networking/cluster-ip-allocation (last accessed on November 11, 2023).

UNIFIED PATENTS EXHIBIT 1010
Page 19 of 19

AA/SWA Ex. 1015, p.259 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Alkhatib	§	Attorney Docket No.: IVI785
	§	
U.S. Patent 7,949,785	§	
	§	
Issue Date: May 24, 2011	§	Customer No.: 165774
	§	
Filing Date: March 31, 2003	§	
	§	
For: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM	§	

REQUEST FOR *EX PARTE* REEXAMINATION OF U.S. PATENT 7,949,785

Mail Stop "*Ex Parte* Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to the provisions of 35 U.S.C. §§ 301-307, Unified Patents, LLC ("Requester") hereby requests an *ex parte* reexamination of claims 30 and 34 (the "Challenged Claims") of U.S. Patent 7,949,785 (the "'785 Patent," Ex. 1001), which issued on May 24, 2011 to Alkhatib from U.S. Patent Application 10/403,818 (the "'818 Application"), filed on March 31, 2003. The '785 Patent does not claim priority to any other domestic or foreign priority date.[1] The '785 Patent is currently assigned to Intellectual Ventures I LLC ("IV" or "Patent Owner"). The assignment is recorded in the U.S. Patent and Trademark Office ("USPTO") at reel/frame 065469/0182.

Requester submits that this Request presents prior art references and analyses that are noncumulative of the prior art that was before the examiner during the original prosecution of the '785 Patent and that the Challenged Claims are invalid over these references. Requester therefore

[1] At this time, Requester assumes March 31, 2003 to be the priority date. Requester reserves the right to challenge the priority date in a different proceeding.

requests that an order for reexamination and an Office Action rejecting claims 30 and 34 be issued.

Ex Parte Patent Reexamination Filing Requirements

Pursuant to 37 C.F.R. § 1.510(b)(l), statements pointing out at least one substantial new question of patentability based on material, non-cumulative reference patents and printed publications for the Challenged Claims of the '785 Patent are provided in Section I of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(2), reexamination of the Challenged Claims of the '785 Patent is requested, and a detailed explanation of the pertinence and manner of applying the cited references to the Challenged Claims is provided in Section II of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(3), copies of every patent or printed publication relied upon or referred to in the statement pointing out each substantial new question of patentability or in the detailed explanation of the pertinence and manner of applying the cited references are provided as Exhibits 1001-1010 and AA of this Request.

Pursuant to 37 C.F.R. §1.510(b)(4), a copy of the '785 Patent is provided as Exhibit 1001 of this Request, along with a copy of any disclaimer, certificate of correction, and reexamination certificate issued corresponding to the patent.

Pursuant to 37 C.F.R. § 1.510(b)(5), the attached Certificate of Service indicates that a copy of this Request, in its entirety, has been served on Patent Owner at the following address of record for Patent Owner, in accordance with 37 C.F.R. § 1.33(c):

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

Also submitted herewith is the fee set forth in 37 C.F.R. § 1.20(c)(1).

Pursuant to 37 C.F.R. § 1.510(b)(6), Requester hereby certifies that the statutory estoppel provisions of 35 U.S.C. § 315I(l) and 35 U.S.C. § 325I(l) do not prohibit Requester from filing this *ex parte* patent reexamination request.

TABLE OF CONTENTS

Table of Exhibits ..... **ii**

I. Substantial New Questions of Patentability **1**

A. U.S. Patent 7,949,785 1

1. Summary 1

2. Prosecution History 6

B. Claim Construction 11

C. Listing of Prior Art Patents and Printed Publications 12

D. Ground 1: *Leung* in view of *Forslöw* and *Mehta* Presents Substantial New Questions of Patentability 13

1. Overview of Prior Art 14

2. Overview of *Mehta* 17

3. Motivation to Modify *Leung* with *Forslöw and Mehta* 18

4. A Finding of a SNQ is Warranted 19

II. Detailed Application of the Prior Art to Every Claim for which Reexamination is Requested **20**

A. Proposed Rejections of the Claims 20

B. Ground 1 (*Leung* in view of *Forslöw and Mehta*) 21

C. Secondary Considerations 22

III. Disclosure of Concurrent Litigation, Reexamination, and Related Proceedings **22**

IV. Conclusion **22**

AA/SWA Ex. 1015, p.262 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

TABLE OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 7,949,785 B2 to Alkhatib (the "'785 Patent")
Ex. 1002	U.S. File History of the '785 Patent ("File History")
Ex. 1003	Declaration of Dr. Michael I. Shamos ("Shamos Decl.")
Ex. 1004	Curriculum Vitae of Dr. Michael I. Shamos
Ex. 1005	U.S. Patent No. 7,036,143 to Leung *et al.* ("Leung")
Ex. 1006	U.S. Patent No. 7,155,518 to Forslöw *et al.* ("Forslöw")
Ex. 1007	U.S. Patent Application Publication No. 2003/0028671 to Mehta *et al.* ("Mehta")
Ex. 1008	U.S. Patent No. 7,290,060 to Kong ("Kong")
Ex. 1009	U.S. Patent No. 7,533,164 to Volz ("Volz")
Ex. 1010	Infringement Claim Chart from *Intellectual Ventures I LLC et al v. Comerica Inc.*, Case No. 2:23-cv-00524, Dkt. 1, Ex. 9 (E.D. Tex. Nov. 15, 2023)
Ex. AA	Claim Chart for Intellectual Ventures I LLC '785 Patent

I. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Prior to describing the substantial new questions of patentability presented in this Request, provided below is an overview of the '785 Patent, a discussion of claim construction, and a summary of the prior art being discussed in the present Request.

A. U.S. Patent 7,949,785

1. Summary

The '785 Patent is generally directed to "[a] private virtual dynamic network … provided for computing devices coupled to public networks or private networks." Ex. 1001 (*'785 Patent*), Abstract. Copies of the '785 Patent and its file history are provided as Exhibits 1001 and 1002, respectively. The claims for which reexamination is requested are reproduced below. Claim 30 is a representative independent claim, so it is used as a starting point. Chaim 34 depend directly from claim 30. All are repeated below.

30. A virtual network manager, comprising:

a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;

a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to:

receive a registration request from an agent associated with a device;

distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and

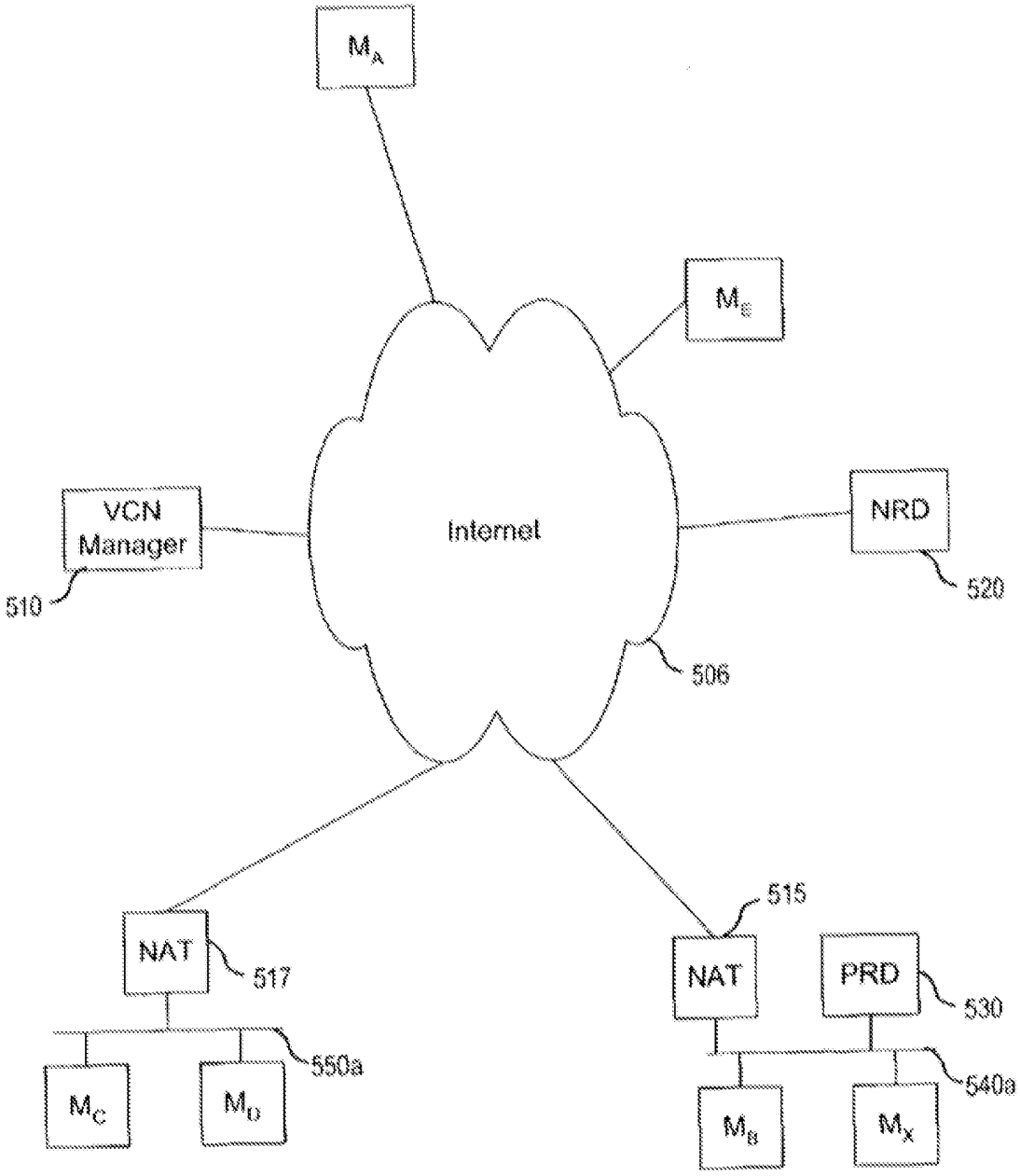
a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.

34. The virtual network manager of claim 30 wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network.

The claims of the '785 Patent are directed to "a virtual network manager" or "a virtual network system" including "a network interface configured for data communication," "a register module configured to register devices in a virtual network," and "a DNS server configured to receive a DNS request … and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device." Ex. 1001 at 36:37-56 (claim 30). The '785 Patent discloses "a secure Virtual Community Network or 'VCN'" in which "all members of the VCN are accessible as if they were part of a physical local network" and "may all make direct connections to each other through communications within the virtual domain." Ex. 1001 at 8:66-9:41. The '785 Patent specifies that "[a] hardware architecture for the machines, server or other devices used to implement the present invention should be well understood to one of average skill in the art" and "[s]uitable hardware includes one or more processors, a memory, a mass storage device, a portable storage device, a first network interface, a second network interface and I/O devices, in communication with each other." Ex. 1001 at 9:42-48. An example of the system is shown in Figure 5A.

AA/SWA Ex. 1015, p.265 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Fig. 5a

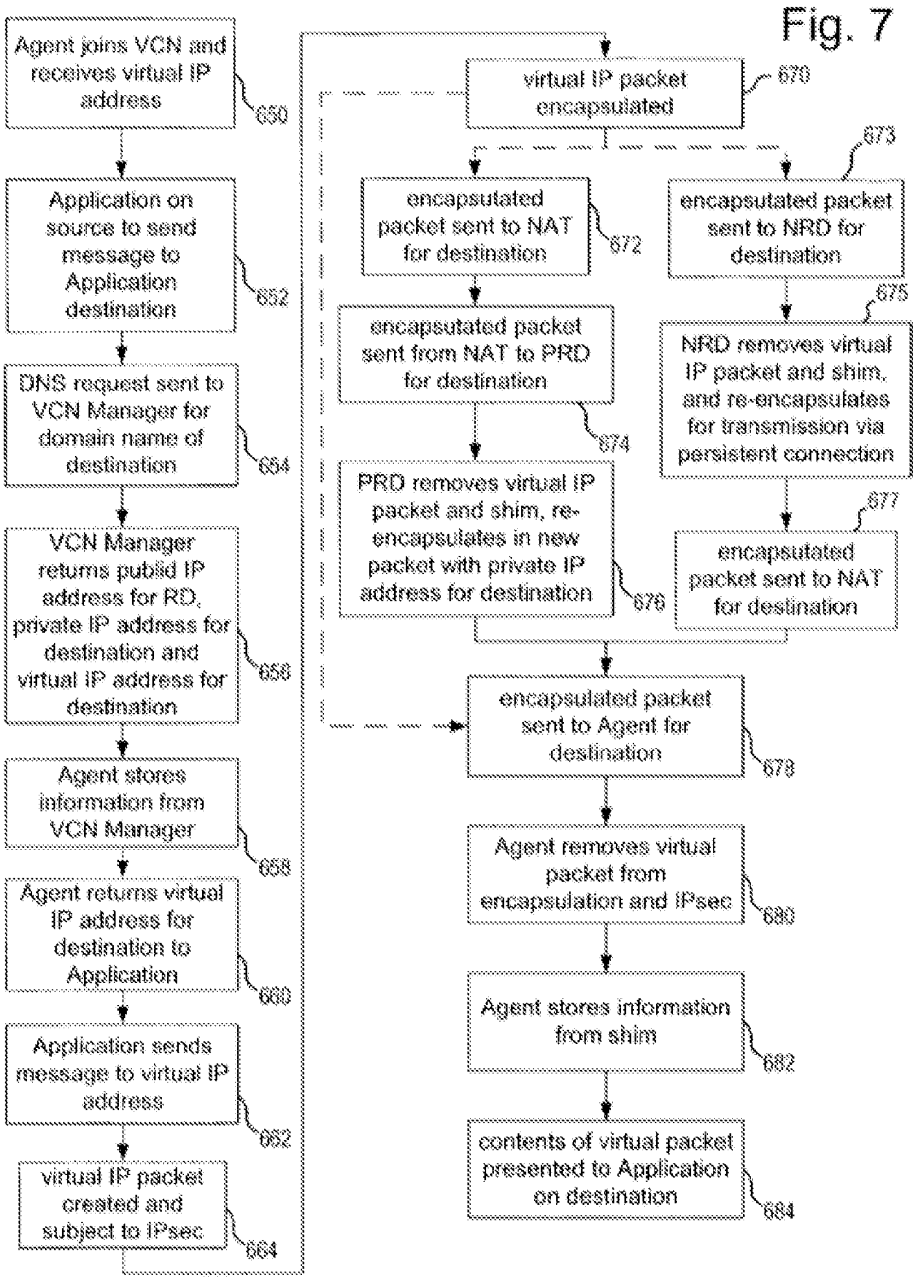

M_A
M_E
VCN Manager
510
Internet
NRD
520
506
515
NAT
517
NAT
PRD
530
550a
540a
M_C
M_D
M_B
M_X

Ex. 1001 at Fig. 5A. The '785 Patent discloses that "[t]he choice of processor is not critical," "the memory can be any conventional computer memory," and "[t]he network interface can include a network card for connecting to an Ethernet or other type of LAN." Ex. 1001 at 9:48-58.

The '785 Patent discloses that "various user machines M_n [are] coupled to the Internet 506, as well as other devices … which implement a virtual community in accordance with the present invention." Ex. 1001 at 10:17-20. "In general, an exemplary system for implementing a VCN in accordance with the invention comprises a VCN Manager 510, a Network Route Director 520 and/or Private Route Director 530, and a number of Member Agents 565." Ex. 1001 at 10:24-27. The '785 Patent notes that "[t]he VCN Manager 510 is a central server or server cluster providing management services, connection services and security services for the VCN." Ex. 1001 at 10:66-11:1.

The '785 Patent discloses that "[i]n order to establish or participate in communication within the VCN, a device must register with and join the VCN, thereby becoming a member of the VCN" and in order to do so, "[t]he Agent will send a message to VCN Manager 510 and receive a virtual IP address back," as shown in step 650 of Figure 7. Ex. 1001 at 14:10-15, Fig. 7.

AA/SWA Ex. 1015, p.267 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786



When the new member device wants to send a message to another device in the VCN, it "will initiate a DNS request" and "[t]his DNS request is sent to the VCN Manager 510," as shown in step 654. Ex. 1001 at 14:32-34. In response to this request, "VCN Manager 510 returns the

public address of the Route Director for the destination, the private address for the destination device and a virtual IP address for the destination device," as shown in Step 656. Ex. 1001 at 14:34-38. "Encapsulated UDP traffic is used by elements of the VCN once membership has been established and the elements are joined in the VCN for management and administrative communications." Ex. 1001 at 11:43-46. *See* Ex. 1003, ¶¶33-36.

The following table summarizes the specification of the '785 Patent:

U.S. Patent 7,949,785	
1:20–24	Field of the Invention
1:25-5:44	Description of the Related Art
5:45–7:60	Summary of the Invention
7:61-8:62	Brief Description of the Drawings
8:64–34:32	Detailed Description of the Present Invention
8:64-10:7	Description of Fig. 4 and overview of the patented VCN system
10:8-11:61	Description of Figs. 5A and 5B and overview of various embodiments of the VCN system
11:62-34:13	Description of Figs. 6A-25 and the communications protocol
34:14-32	Describing breadth of disclosure not limited to described embodiments
34:34-42:31	Listing of Claims 1–90

2. Prosecution History

The '818 Application was filed on March 31, 2003 with 109 proposed claims. In an office action on November 22, 2006, all claims were rejected as anticipated by US Patent Publication No. 2003/0041136 (Cheline). Ex. 1002 at 143-162. On March 22, 2007, the applicant filed a response along with a series of amendments. Ex. 1002 at 170-192. The applicant amended the earlier filed claims by adding elements specifying that the network traffic router "uses router data to route traffic between members of the virtual community" and that "a first member of the virtual community communicates with another member in the virtual community by querying the DNS server to determine a virtual network address and a private network address for the another member, and to determine a public address of the network traffic router." Ex. 1002 at 172-187. In its remarks, the applicant argued that "Cheline can hardly be considered to be a management device for a virtual community" and "the client 102(1) of Cheline does not communicate with the DNS server 120 to obtain a virtual network address and private network address of another client such as client 102(2) and to obtain a public network address of the service provider system 146,

which is asserted by the Examiner to be a network traffic router as claimed.". Ex. 1002 at 190-191.

A final office action was issued on June 5, 2007 rejecting claims 93-100 and 102-109 for the same reasons as the previous office action and claims 1-92 as obvious over Cheline in view of US Patent Publication No. 2004/0006708 (Mukherjee). Ex. 1002 at 202-213. The examiner found that Mukherjee teaches "at least one route director capable of communicating with users in the user set, the at least one route director routes traffic between the users," among other things. Ex. 1002 at 207-208. On November 5, 2007, the applicant responded by attempting to traverse the rejections. Ex. 1002 at 217-234. Specifically, the applicant argued the "Office Action does not address the amended claims." Ex. 1002 at 233.

The examiner then issued an Advisory Action Before Filing of an Appeal Brief on November 19, 2007. Ex. 1002 at 240-242. The applicant then filed a Request for Continued Examination (RCE) containing some minor amendments and arguments. Ex. 1002 at 243-267.

On February 13, 2008, the examiner issued another office action stating that the amendments were non-responsive. Ex. 1002 at 305-308. The applicant responded by heavily amending the claims to entirely rewrite them. Ex. 1002 at 309-372. For example, claim 32 and 44 (which eventually were combined into issued claim 30) were amended as follows:

AA/SWA Ex. 1015, p.270 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

32. (currently amended) A ~~system~~ virtual network manager, comprising:

a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;

a register module configured to register devices in a virtual network, the register module further configured to:

receive a registration request from an agent associated with a device; and

distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address.

~~a management device for a virtual community, the management device including a network interface coupled to a public address realm and having a public address; and~~

~~a network traffic router which uses router data to route traffic between members of the virtual community, the router data including at least one association of a logical identifier with public routing information for a member.~~

44. (currently amended) The ~~system~~ virtual network manager of claim 32 further comprising a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device. ~~wherein each member receives a respective virtual network address when registering with the management device to join the virtual community, the management device includes a DNS server for the virtual community, a first member in the virtual community communicates with another member in the virtual community by querying the DNS server to determine a private network and the respective virtual network address for the another member, and to determine a public address of the network traffic router, and the first member communicates with the another member using an encapsulated packet having a source address which is the respective virtual network address of the first member and a destination address which is the respective virtual network address of the another member, by sending the encapsulated packet to the network traffic router in an encapsulating packet having a destination address which is the public address of the network traffic router, the private network address for the another member is included in the encapsulating packet and is used by the network traffic router to route the encapsulated packet to the another member.~~

Further, the applicant argued that "Cheline and/or Mukherjee do not teach a virtual network address, or a device being identified in a virtual network by a virtual network address, as recited in claim 32." Ex. 1002 at 347.

On February 4, 2009, another office action was issued rejecting all pending claims under 35 U.S.C. 101 and most claims as anticipated by or obvious over US Patent Publication No.

2008/0232295 (Kreiner). Ex. 1002 at 391-400. Claims 16 and 44 were objected to as dependent upon a rejected base claim, but "would be allowable if rewritten in independent form." Ex. 1002 at 399. The examiner provided that "[t]he prior art does not teach he *[sic]* claimed relation between the elements claimed" as the reason for the indication of allowable subject matter. *Id.*

On May 29, 2009, the applicant responded to the office action by amending independent claims 1 and 32 to incorporate the subject matter of claims 16 and 44 and by amending the other independent claims in similar ways. Ex. 1002 at 437-465.

On November 29, 2009, the examiner issued another office action stating that certain of the amendments were non-responsive. Ex. 1002 at 489-492. The applicant responded on October 24, 2009 with mostly identical amendments, but including arguments regarding claim 93. Ex. 1002 at 493-521. On February 5, 2010, the examiner issued a Notice of Non-Compliant Amendment (Ex. 1002 at 528-530) and the applicant responded on February 22, 2010 by correcting the amendments to only show claim 93 as currently amended. Ex. 1002 at 531-559. On June 1, 2010, the examiner issued another Notice of Non-Complaint Amendment related to the markings of claim 93 (Ex. 1002 at 579-581) and the applicant responded on June 7, 2010 by correcting the amendment to claim 93. Ex. 1002 at 582-610.

On September 1, 2010, the examiner issued another office action stating that claims 1-15, 17-24, 26-36, 41-43, and 93-109 were allowed and claims 53-66 and 68-92 were rejected as anticipated by US Patent No. 6631416 (Bendinelli). Ex. 1002 at 613-618. The examiner provided as reasons for allowance that "the prior art was not found to teach or suggest returning a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device in response to a DNS request in the context of claims 1, 32, and 93" and "[s]pecifically, **no examples were found in the prior art of record in which both a private address and a virtual address of a destination device would be returned.**" Ex. 1002 at 616-617. The applicant responded on October 21. 2010 by amending claims 53-55, 64, and 80 to include a similar DNS request and response element. Ex. 1002 at 658-683.

On November 5, 2010, the examiner issued another office action rejecting claims 1-15, 17-24, 26-36, 41-43, and 80-92 as invalid under 35 U.S.C. 101, but otherwise containing allowable subject matter. Ex. 1002 at 687-691. The applicant responded on December 2, 2010 by amending

AA/SWA Ex. 1015, p.273 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

those claims "to clarify that the recited virtual network manager and/or route director are implemented with a memory and a processor of a computing device." Ex. 1002 at 723-750. For example, claim 32 was amended as follows:

> **32. (currently amended)** A virtual network manager, comprising:
>
> a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;
>
> a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to:
>
> receive a registration request from an agent associated with a device;
>
> distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and
>
> a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.

The examiner issued a Notice of Allowance on January 14, 2011. Ex. 1002 at 760-766. *See* Ex. 1003, ¶¶37-46.

B. Claim Construction

The claims must be given their "broadest reasonable interpretation consistent with the specification." *See* MPEP § 2258; *In re Yamamoto*, 740 F.2d 1569, 222 USPQ 934 (Fed. Cir. 1984). This Request presents its claim analysis in a manner that is consistent with the broadest

AA/SWA Ex. 1015, p.274 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

reasonable interpretation consistent with the specification. Requester does not believe any specific terms of the '785 Patent require construction beyond their plain and ordinary meaning. Requester reserves the right to advocate different claim interpretations in any other forum or proceeding if necessary.

C. Listing of Prior Art Patents and Printed Publications

Reexamination of the Challenged Claims is requested in view of the following references:

- **Ex. 1005 ("Leung")**: U.S. Patent No. 7,036,143 to Leung *et al.* was filed on September 19, 2001 and issued on April 25, 2006. *Leung* is prior art at least under 35 U.S.C. § 102(e).
- **Ex. 1006 ("Forslöw")**: U.S. Patent No. 7,155,518 to Forslöw was filed on January 8, 2001 and issued on December 26, 2006. *Forslöw* is prior art at least under 35 U.S.C. § 102(e).
- **Ex. 1007 ("Mehta")**: U.S. Patent Publication No. 2003/0028671 to Mehta *et al.* was filed on June 10, 2002 and published on February 6, 2003. *Gunn* is prior art at least under 35 U.S.C. § 102(e).

Neither Leung nor Mehta were cited during prosecution of the '785 Patent and Forslöw (via an earlier publication) was merely cited in a list of references on a Notice of References Cited. *See* Ex. 1002 at 167. A Form SB-08 and copies of the cited references are submitted herewith. This request is also supported by the declaration of Dr. Michael I. Shamos (Ex. 1003). *See* Ex. 1003, ¶¶1-62. To the extent that additional references are discussed in Dr. Shamos' declaration, copies of these additional references are also being submitted, and are included on Form SB-08.

As shown below, Requester submits that the prior art references raise a new "substantial question of patentability" because "the teaching of the (prior art) patents and printed publications is such that a reasonable examiner would consider the teaching to be important in deciding whether or not the claim is patentable." *See* MPEP § 2242. For example, the references discussed below and in further detail in the attached charts, when considered as an ordered combination, teach each limitation of the Challenged Claims, including the idea of "*register[ing] devices in a virtual network*" by "*distribut[ing] a virtual network address to the device*" and a "*DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second*

AA/SWA Ex. 1015, p.275 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

device in the virtual network, and a virtual network address associated with the second device." Ex. 1001 at Claim 30.

Further, they are new. These references were not previously considered; the "same question of patentability as to the claim has not been decided by the Office in an earlier concluded examination or review of the patent" at least because neither Leung nor Mehta was before the Office during prosecution of the '785 Patent and Forslöw was merely cited in a list of references contained in a Notice of References Cited and none of the prior art references relied upon in this request were before the office during a prior post-grant proceeding challenging any claim of the '785 Patent, any of which that are known to Requester have been listed below in Section III, *infra*.

D. Ground 1: *Leung* in view of *Forslöw* and *Mehta* Presents Substantial New Questions of Patentability

As shown below, Requester submits that *Leung* in view of *Forslöw* and *Mehta* raises a new "substantial question of patentability" as to claims 30 and 34 because "the teaching of the (prior art) patents and printed publications is such that a reasonable examiner would consider the teaching to be important in deciding whether or not the claim is patentable." *See* MPEP § 2242. For example, the references discussed below and in further detail in the attached chart (*see* Exhibit AA), when considered as an ordered combination, teach each limitation of the claims, including "*register[ing] devices in a virtual network*" by "*distribut[ing] a virtual network address to the device*" and a "*DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device*." Further neither *Leung* nor *Mehta* were previously considered during prosecution, and, therefore, the "same question of patentability as to the claim has not been decided by the Office in an earlier concluded examination or review of the patent" at least because most of the art referenced in this Ground was not before the Office during prosecution of the '785 Patent or during a prior post-grant proceeding challenging any claim of the '785 Patent, any of which that are known to Requester have been listed in the attached Information Disclosure Statement ("IDS"), Form SB-08. *See id.*

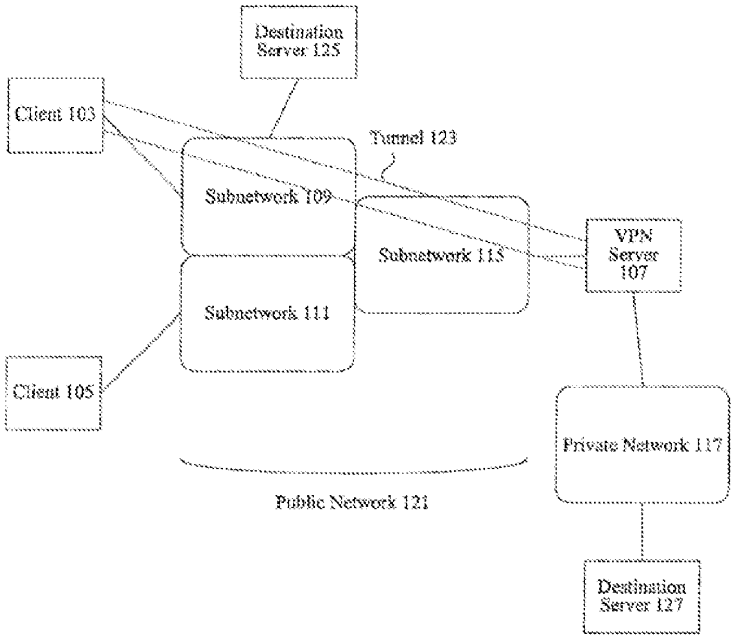
AA/SWA Ex. 1015, p.276 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

1. Overview of Prior Art

a. Overview of *Leung*

Leung (**Ex. 1005,** U.S. Patent No. 7,036,143) discloses a virtual private network system in which "the VPN client can establish sessions with a variety of destination nodes including destination nodes on a private or enterprise network associated with the VPN server." Ex. 1005 (*Leung*), Abstract. This system is shown in Figure 1.

Figure 1

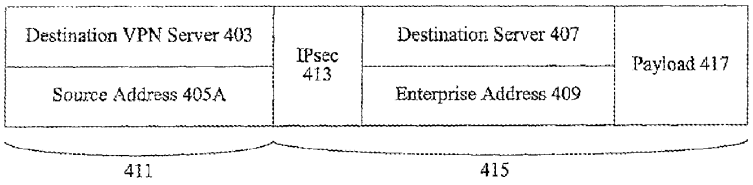


Id. at Fig. 1.

Leung discloses that "the public network 121 is connected to private network 117 through a VPN server 107." *Id.* at 4:57-64. *Leung* discloses that "the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general purpose computing device." *Id.* at 11:12-17. *Leung* discloses that "[t]o acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107," including "information such as its

subnetwork address, its user name, and its password." *Id.* at 5:11-18. In response, the VPN server provides the client with an "enterprise address," which "is the address that the VPN client users to communicate with other nodes such as nodes in the company private network." *Id.* at 4:5-10. *Leung* explains that "other nodes including nodes in the company private network will see the VPN client as having the enterprise address, and will therefore communicate with the VPN client via the enterprise address." *Id.* at 4:12-25. Upon receiving the enterprise address, the client can communicate via a VPN tunnel via encapsulated packets. For example, "the encapsulated portion 415 preferably contains the enterprise address 409 allocated by the VPN server to the VPN client during the creation of the VPN tunnel, which may be used to authenticate the sender," as shown in Figure 4A. *Id.* at 6:53-67.

Figure 4A

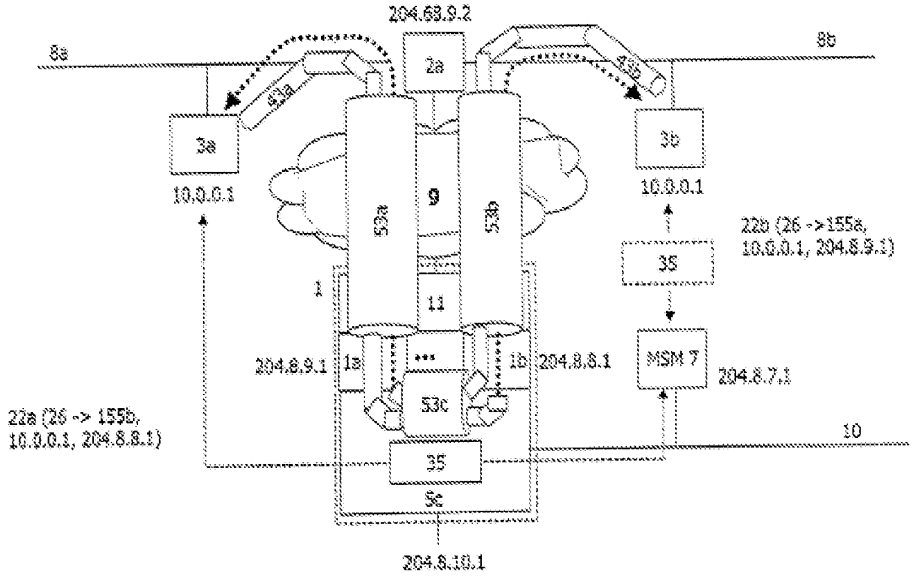


Id. at Fig. 4A. *See, e.g.,* Ex. 1003, ¶¶47-50.

a. Overview of *Forslöw*

Forslöw **(Ex. 1006,** U.S. Patent No. 7,155,518) discloses "a network-based mobile workgroup system showing a selected set of users from two or more mobile virtual private networks to form an extranet workgroup in a secure manner." Ex. 1006 (*Forslöw*), Abstract. *Forslöw* discloses that its "system also entails a mobile service manager that has a public IP address and a set of mobile nodes that all have a UFQDN (user fully qualified domain name) within the overall mobile workgroup system." *Id.*, Abstract. This system is shown in Figure 2.

Fig. 2



Id. at Fig. 2. "FIG. 2 shows the tunnel structure that is established in order to allow two mobile nodes 3a and 3b to be part of the same extranet workgroup in a secure manner." *Id.* at 9:62-10:6.

Forslöw discloses that backbone virtual home agent 5c "act[s] as the common gateway towards the Internet 6 for all virtual home agents 1a and 1b" and "also hosts a management network 10 to which a mobile service manager 7 for the mobile workgroup system is attached." *Id.* at 9:30-43. "The mobile nodes 3a and 3b that are belonging to an extranet workgroup retrieve a list of workgroup members 26 by doing HTTPS requests 22a and 22b to the mobile service manager 7," which functions as a DNS server. *Id.* at 10:7-20. These requests are sent to the mobile service manager 7 and it returns "a triplet including the user fully qualified domain name 155 b/155 a, the mobile node 3 private IP address 156 a/b (10.0.0.1) and the virtual home agent's 1 a/1 b public IP address 157 a/b (204.8.9.1 and 204.8.8.1 respectively)." *Id.*; *see also id.* at 11:9-17. 11:18-28. *Forslöw* further discloses that "[t]he center module of a virtual home agent 1a/b is the virtual router 5 a/b," which "is making nexthop decisions for datagrams passing through the virtual home agent

1 a/b." *Id.* at 12:14-21. *See, e.g.*, Ex. 1003, ¶¶51-52.

2. Overview of *Mehta*

Mehta (**Ex. 1007**, U.S. Patent Publication No. 2003/0028671) discloses a system "for initiating communication with a device on a private network from a device on a public network to achieve virtual end-to-end connectivity." Ex. 1007 (*Mehta*) at [0002]. Figure 2 provides an example of *Mehta*'s system.

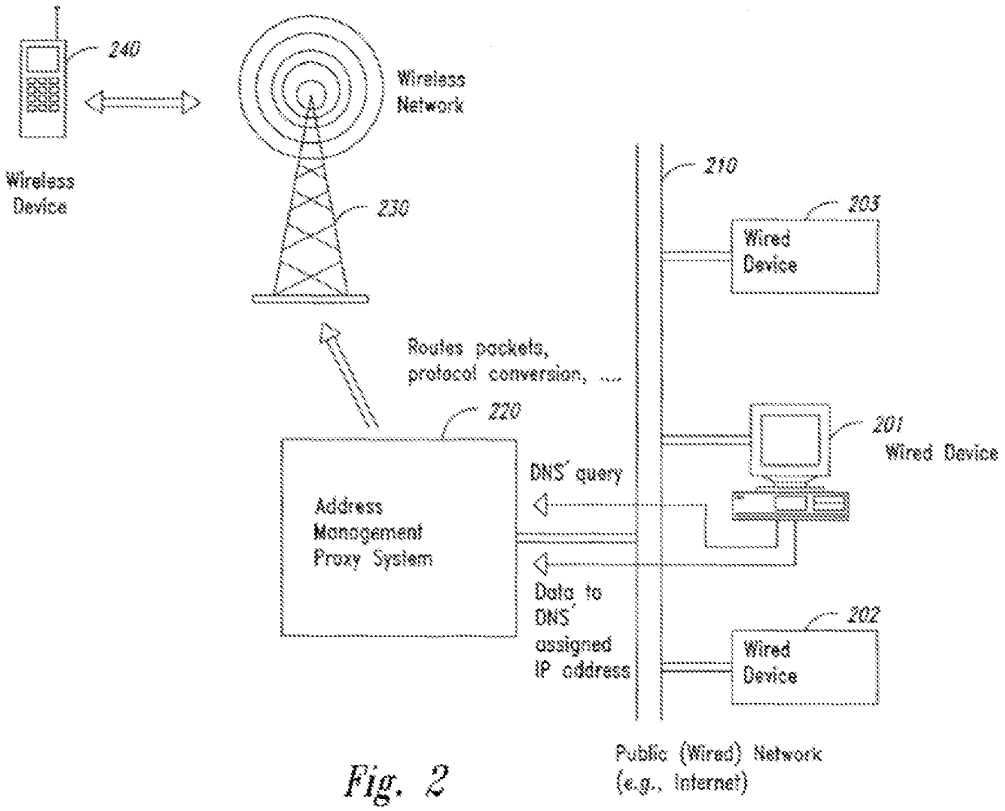


Fig. 2

Ex. 1007 at Fig. 2.

Mehta discloses example embodiments that provide "an Address Management Proxy System ("AMPS"), which enables devices and systems connected to a public internetwork, such as the Internet, to initiate communication with and send data to wireless devices connected to a private wireless network." Ex. 1007 at [0011]. *Mehta* discloses that "the AMPS comprises one or more modified DNS/API servers, one or more Address Proxy/Routers, an Address Management Data Server, one or more Address Management Data Repositories, and optionally a load balancer."

Id. at [0012]. "The AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device, and returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device." *Id.* *Mehta* discloses that this "temporary public address is, for example, an address associated with one of the Address Proxy/Routers, which are connected to the external public network and have access to the private addresses on the private wireless network" and that it "is then usable by the device on the externsal public network to send data to the wireless device." *Id.*

More specifically, "the wired device 201 performs a query (for example, a modified DNS query) to locate a routable public address that corresponds to wireless device 240" and then "[t]he Address Management Proxy System 220 receives the query and determines and assigns a public (routable) address from a pool of addresses, which address can be used as a destination address for data packets targeted to wireless device 240." *Id.* at [0031]. At that point, "[d]ata is sent to a particular Address Proxy/Router because the public (routable) address of that Address Proxy /Router was returned to the requesting/ source device in response to a query of the DNS'/API server of the AMPS." *Id.* at [0058]. *See, e.g.,* Ex. 1003, ¶¶53-55.

3. Motivation to Modify *Leung* with *Forslöw and Mehta*

It would have been obvious to a POSITA to incorporate *Forslöw*'s and *Mehta*'s teachings related to a communication across virtual networks into *Leung*'s virtual private network system. Ex. 1003, ¶¶56-61. *Leung* discloses a VPN system in which client devices gain access to the VPN in order to send data to devices within the VPN. See, e.g., Ex. 1005, 5:8-18. *Forslöw* discloses a similar VPN, but specifically goes into detail in describing the way in which the DNS server (which it calls a mobile service manager) facilitates communication over the VPN system. See, e.g., Ex. 1006, 9:62-10:20. A POSITA would have been motivated to make such a combination because implementation of *Forslöw*'s VPN tunnelling system would have allowed data messaging to be sent in a more efficient and secure manner. Ex. 1003, ¶56.

Additionally, *Forslöw*'s VPN system provides for a virtual route director to assist in data mapping. See, e.g., Ex. 1006, 9:19-29. *Mehta* discloses a similar virtual networking system that operates with a DNS server and a route director, but it goes into more details about the operation of the route director, and thus provides for such DNS servers to provide private to network address associated with a network address proxy machine. See, e.g., Ex. 1007, [0012], [0031]-[0032]. A

AA/SWA Ex. 1015, p.281 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

POSITA would have been motivated to make this combination because implantation of *Mehta*'s utilization of the DNS server would have aided in the security of the VPN system created by the combination of *Leung* and *Forslöw*. Ex. 1003, ¶57.

Furthermore, a POSITA would have been motivated to combine *Leung, Forslöw*, and *Mehta* because the combination merely uses a known technique to improve similar devices in the same way. See *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 401 (2007). For instance, the combination would have merely required the use of a known technique, specifically the utilization of routing via addresses provided by a DNS server to similar VPN systems in the same way. Ex. 1003, ¶58 (*citing* Ex. 1008 (Kong), 2:15-42, 5:17-546:5 and Ex. 1009 (Volz) at 5:13-26, 11:31-64, 19:47-20:15).

A POSITA would have had a reasonable expectation of success in modifying *Leung*'s VPN system, which allows for registration and data transmission by client devices, to perform this data transmission via use of a DNS server and route director, as taught by *Forslöw* and *Mehta*, because doing so would merely have implemented a well-known technique in the VPN system of *Leung*, as shown in Exhibit AA. Ex. 1003, ¶59.

Leung combined with *Forslöw* and *Mehta* teaches every limitation of every Challenged Claim. As mentioned, a POSITA would have been motivated to combine, and would have had a reasonable expectation of success in combining, *Forslöw's* and *Mehta's* teachings related to the use of a DNS server in a virtual network system with Leung's teaching related to a VPN system. Ex. 1003, ¶¶56-61. Thus, *Leung*, in combination with *Forslöw* and *Mehta*, renders the Challenged Claims obvious.

4. A Finding of a SNQ is Warranted

For the reasons outlined in Section II.B, *infra*, and in accompanying Exhibit AA, the combination described for Ground 1 presents a substantial new question of patentability as to claims 30 and 34, and further demonstrate that any allegedly novel features of the '785 Patent (e.g., a DNS server that returns return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device), were well known in the art and disclosed by the references in this Request. For example, *Leung* discloses a "VPN server" that registers devices and provides the client with an "enterprise address," which "is the address that the VPN client

users to communicate with other nodes such as nodes in the company private network." Ex. 1005 at 4:5-10.

Further, *Forslöw* discloses a similar VPN system in which a mobile service manager 7 (i.e., a DNS server) receives HTTPS requests and returns a triplet, including a mobile node private IP address 156b (i.e., a private network address associated with a second device in the virtual network) and a virtual home agent's 1b public IP address 157b (i.e., a virtual network address associated with the second device. Ex. 1006 at 9:62-10:6, 10:7-20, 11:9-28, Fig. 2.

In addition, *Mehta* discloses a similar virtual networking system in which an "AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device, and returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device" and is "an address associated with one of the Address Proxy/Routers" (i.e., route directors). Ex. 1006 at [0012].

A reasonable Examiner would consider the combined teachings of these references important in determining whether claims 30 and 34 are patentable because the proposed combination was never considered during prosecution of the '785 Patent. Section II below and Exhibit AA demonstrate in greater detail how the combination of *Leung, Forslöw,* and *Mehta* discloses or renders obvious each and every limitation of the Challenged Claims.

II. DETAILED APPLICATION OF THE PRIOR ART TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED

A. Proposed Rejections of the Claims

The present Request presents multiple proposed obviousness rejections of the Challenged Claims based on *Leung*, *Forslöw*, and *Mehta*.

Requester notes that the proposed rejections below are based on obviousness under 35 U.S.C. § 103(a) in light of the knowledge of a person of ordinary skill in the art at or around March 31, 2003 (a "POSITA"). The level of ordinary skill in the art that one would need in order to have the capability of understanding the scientific and engineering principles applicable to the '785 Patent is (i) a Bachelor's degree (or higher degree) in computer science or equivalent and (ii) at least two years of experience working in the fields of virtual networking. Ex. 1003, ¶¶28-30. When compared with the prior art described below and in light of the knowledge of a POSITA, any

"differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art." 35 U.S.C. § 103 (pre-AIA). The proposed rejections are listed below and are described in further detail in the attached claim charts. *See* Exhibit AA.

Proposed Rejection 1 (Ground 1)	Leung in view of Forslöw and Mehta renders claims 30 and 34 as obvious under 35 U.S.C. § 103

B. Ground 1 (*Leung* in view of *Forslöw and Mehta*)

Leung in view of *Forslöw* and *Mehta* renders obvious each and every element of claims 30 and 34. *See* Ex. 1003, ¶¶28-30. For ease of reference, Requester outlines examples from each reference that disclose or render obvious each associated claim limitation below. Further, a framework for a POSITA's background knowledge and motivations to combine are provided by Requester's expert, Dr. Michael I. Shamos (*see* Ex. 1003, ¶¶1-62). A more detailed mapping of Ground 1 is provided in Exhibit AA.

Regarding claim 30, *Leung* in view of *Forslöw* and *Mehta* renders obvious ***[a] virtual network manager, comprising*** (although the preamble may not be limiting; *see Leung* at 4:57-64, Fig. 1)***: a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address*** (*see e.g., Leung* at 1:12-15, 11:12-17, 11:39-51, 11:20-28, 4:59-60, 4:66-5:11, 4:57-64, Figs. 1, 10 and *Forslöw* at Abstract)***; a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to*** (*see e.g., Leung* at 11:19-37, 4:66-5:11, 5:8-16, Fig. 10)***: receive a registration request from an agent associated with a device*** (*see e.g., Leung* at 5:11-18, 4:67-5:3, Fig. 1)***; distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and*** (*see e.g., Leung* at 4:5-10, 4:12-25, 5:13-26, 6:53-67, 6:41-43, 7:1-30, 8:1-9:23, 9:52-10:21, Figs. 1, 4, 5, 8) ***a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device*** (*see e.g., Forslöw* at 9:62-10:6, 9:30-43, 10:7-

20, 10:54-64, 11:9-17, 11:18-28, 12:14-21, 15:57-65, Fig. 2 and *Mehta* at [0012], [0031], [0032], [0057], [0058], Fig. 7).

Regarding claim 34 (which depends from claim 30), *Leung* in view of *Forslöw* and *Mehta* renders obvious ***virtual network manager of claim 30 wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network*** (see e.g., *Leung* at 5:11-18, 4:67-5:3, 6:53-67, 6:41-43, Figs. 1, 4A).

C. Secondary Considerations

This Request demonstrates that the Challenged Claims of the '785 Patent are unpatentable as obvious in view of the prior art references. The Applicant did not identify any evidence of secondary considerations during prosecution. Further, the clear teachings in the prior art cannot be overcome by any supposed "secondary considerations." *Shamos Decl.* (Ex. 1003), ¶¶22-24; *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 36 (1966).

III. DISCLOSURE OF CONCURRENT LITIGATION, REEXAMINATION, AND RELATED PROCEEDINGS

Based on information available to Requester, the '785 Patent is the subject of four District Court litigations, as listed in the below table. Requester is unaware of any prior reexaminations or other post-grant proceedings in which the '785 Patent is or has been involved.

- *Intellectual Ventures I LLC et al v. JP Morgan Chase & Co.*, Case No. 2:23-cv-00523 (E.D. Tex. Nov. 15, 2023);
- *Intellectual Ventures I LLC et al v. Liberty Mutual Holding Company Inv. et al*, Case No. 2:23-cv-00525 (E.D. Tex. Nov. 15, 2023);
- *Intellectual Ventures I LLC et al v. Comerica Inc.*, Case No. 2:23-cv-00524 (E.D. Tex. Nov. 15, 2023);
- *Assurant v. Intellectual Ventures I LLC et al*, Case No. 1:24-cv-00344 (D. Del. Mar. 15, 2023).

IV. CONCLUSION

The Commissioner is hereby authorized to charge Deposit Account 50-6990 under Docket No. IVI785 the *Ex Parte* Reexamination fee of $12,600 under 37 C.F.R. § 1.20(c)(1). Requester

believes no other fee is due with this submission, however the Commissioner is hereby authorized to charge any fee deficiency or credit any over-payment to Deposit Account 50-6990.

Please direct all correspondence in this matter to the undersigned.

Dated: May 22, 2024

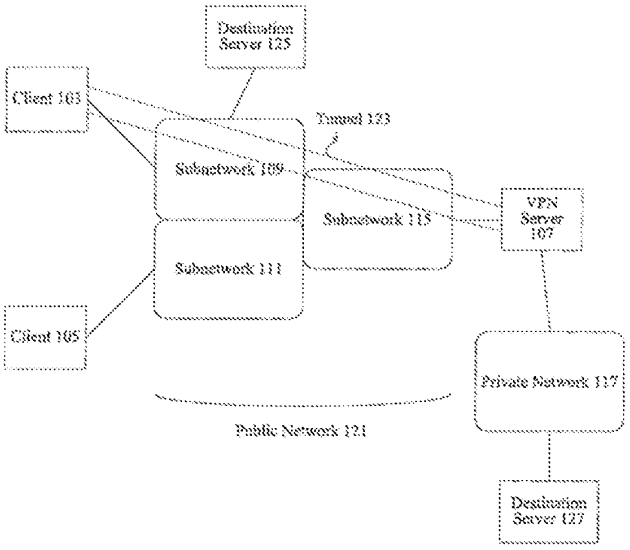
Respectfully submitted,

By: /Jordan M. Rossen/
Jordan M. Rossen (Reg. No. 74,064)
Alyssa Holtslander (Reg. No. 64,026)
Unified Patents, LLP
4445 Willard Ave., Suite 600
Chevy Chase, MD 20815
jordan@unifiedpatents.com
T: 202.701.1850
alyssa@unifiedpatents.com

Attorneys for Requester
Unified Patents, LLC

AA/SWA Ex. 1015, p.286 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

EXHIBIT AA
Claim Chart for
Intellectual Ventures I LLC '785 Patent

US 7,949,785	US 7,036,143 (*Leung*) US 7,155,518 (*Forslöw*) US 2003/0028671 A1 (*Mehta*)
	Claim 30
[30.0] A virtual network manager, comprising:	*Leung* discloses *a virtual network manager* (e.g., a VPN server). ● FIG. 1 is a diagrammatic representation of a system in which embodiments of the present invention may be implemented. The subnetworks 109, 111, and 115 are part of a public network 121. The public network 121 can be connected with a variety of private networks as well as other public networks through different network nodes. **For example, the public network 121 is connected to private network 117 through a VPN server 107**. o 4:57-64 Figure 1  o Fig. 1
[30.1] a network interface	*Leung* discloses *a network interface* (e.g., interfaces 1068) *configured for data communication* (e.g., control the sending and receiving of data packets

configured for data communication via a virtual network that is defined by a domain name having an associated public network address;	over the network) *via a virtual network* (e.g., a public network) *that is defined by a domain name having an associated public network address* (e.g., a subnetwork address from the Internet service provider associated with the subnetwork). ● Conventional **virtual private networks deployed on a public network infrastructure** provide clients the same security, management, quality of service policies, and benefits provided to clients in private networks. o 1:12-15 ● The present invention may be implemented on a general-purpose network host machine such as a personal computer or workstation. Further, **the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general purpose computing device**. o 11:12-17 ● The **interfaces 1068 are typically provided as interface cards** (sometimes referred to as "line cards"). **Generally, they control the sending and receiving of data packets over the network and sometimes support other peripherals used with the router 1010.** Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided such as fast Ethernet interfaces, Gigabit Ether net interfaces, ATM interfaces, HSSI interfaces, POS inter faces, FDDI interfaces and the like. Generally, these inter faces may include ports appropriate for communication with the appropriate media. o 11:39-51 ● FIG. 10 is a diagrammatic representation of a general purpose computing device that can be used. The **computing system 1010 suitable for implementing the present invention includes a master central processing unit (CPU) 1062, interfaces 1068,** and a bus 1015 (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU 1062 is responsible for tasks such as acquiring a subnetwork address or assigning an address to a TCP/IP stack. o 11:20-28

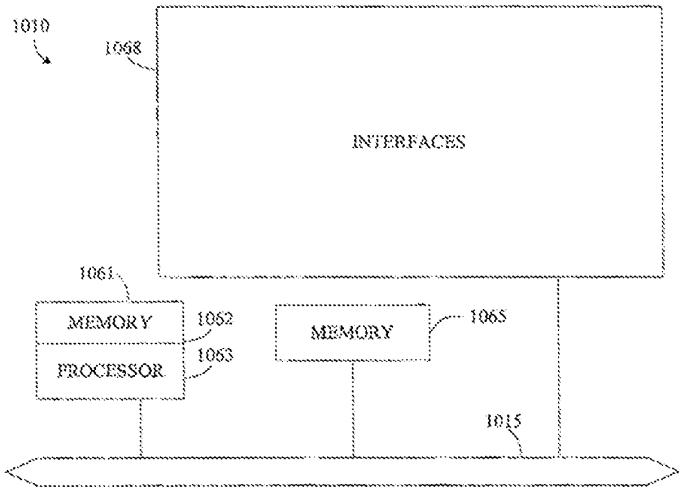


Figure 10

- Figure 10

- The subnetworks 109, 111, and 115 are part of a public network 121.
  - 4:59-60

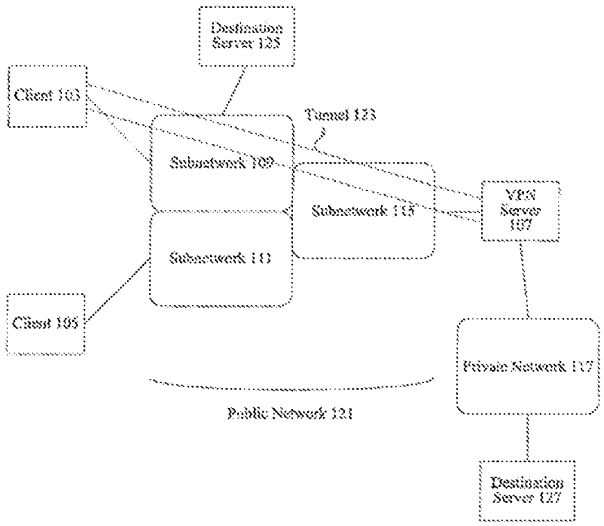
- The **public network 121 is also connected to a destination server 125 as well as clients 103 and 105**. In one example, a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 107. For instance, **client 103 may be connected to public network 121 through an Internet service provider. In this example, client 103 may acquire a subnet work address from the Internet service provider associated with subnetwork 109**. When the subnetwork address is obtained, the subnetwork address may be specifically associated with subnetwork 109. Using the subnetwork address, client 103 can access a destination server 125 in a public network 121.
  - 4:66-5:11

- FIG. 1 is a diagrammatic representation of a system in which embodiments of the present invention may be implemented. The subnetworks 109, 111, and 115 are part of a public network 121.

The public network 121 can be connected with a variety of private networks as well as other public networks through different network nodes. For example, the public network 121 is connected to private network 117 through a VPN server 107.

- 4:57-64

Figure 1



- Fig. 1

A POSITA would have understood that the subnetwork address obtained from the Internet service provider disclosed in *Leung* is based on the domain name of the public network. Ex. 1003, ¶48. However, to the extent it is determined that *Leung*'s *virtual network* (e.g., a public network) is not *defined by a domain name having an associated public network address*, it would have been obvious for *Leung*'s virtual network to have been defined by a domain name. A POSITA would have understood that *Leung*'s VPN server would generally correspond to a domain name. *Id.*

Furthermore, to the extent it is argued that *Leung*'s virtual network is not defined by a domain name, a POSITA would have been motivated to combine *Leung*'s virtual networking system with *Forslöw's* virtual networking system, as explained in the Request for *Ex Parte* Reexamination at Section I.D.3 and with respect to element [30.3], below.

	Ex. 1003, ¶¶56-61. In addition, a POSITA would have been motivated to modify the virtual network of *Leung* to incorporate the property of the virtual network of *Forslöw*, in that it is defined by a user fully qualified domain name (UFQDM). Ex. 1003, ¶60. This is true because a POSITA would have understood that *Leung*'s virtual network requires knowledge of such a domain name to access the VPN server. *Id.* Thus, a POSITA would have looked to a system, such as *Forslöw*, which explicitly explains that such a virtual network would have been defined by a particular type of domain name, i.e., a user fully qualified domain name. *Id.* *Forslöw* discloses *a virtual network* (e.g., a mobile virtual network) *that is defined by a domain name having an associated public network address* (e.g., a user fully qualified domain name). ● The present invention describes a network-based mobile workgroup system allowing a selected set of users from two or more **mobile virtual private networks** to form an extranet workgroup in a secure manner. The invention is based on the limited private address scenario, which entitles mobile nodes having private, possibly overlapping, addresses as defined in RFC 1918, while **home and foreign agents have public IP addresses. Each home agent is dedicated to one mobile virtual private network (M-VPN), while a foreign agent may be shared by multiple M-VPNs. The system also entails a mobile service manager that has a public IP address and a set of mobile nodes that all have a UFQDN (user fully qualified domain name) within the overall mobile workgroup system.** ○ Abstract
[30.2] a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to:	*Leung* discloses *a memory* (e.g., memory 1061) *and a processor* (e.g., CPU 1062) *to implement a register module configured to register devices in a virtual network,* (e.g., may be responsible for maintaining associations between clients and enterprises). ● A VPN client or a VPN server can be implemented on a general purpose computing device. FIG. 10 is a diagrammatic representation of a general purpose computing device that can be used. The computing system 1010 suitable for implementing the present invention includes **a master central processing unit (CPU) 1062, interfaces 1068, and a bus 1015 (e.g., a PCI bus).** When acting under the control of appropriate software or firmware, the **CPU 1062 is responsible for tasks such as acquiring a subnetwork address or assigning an address to a TCP/IP stack. On the VPN server side, the CPU 1062 may be responsible for maintaining associations between clients and enterprises. The**

CPU 1062 may be a general purpose processor or it may be specially designed hardware for implementing a VPN client or a VPN server. In a specific embodiment, a memory 1061 (such as non-volatile RAM and/or ROM) also forms part of CPU 1062. However, there are many different ways in which memory could be coupled to the system. Memory block 1061 may be used for a variety of purposes such as, for example, caching and/or storing data, programming instructions, etc.

- 11:19-37

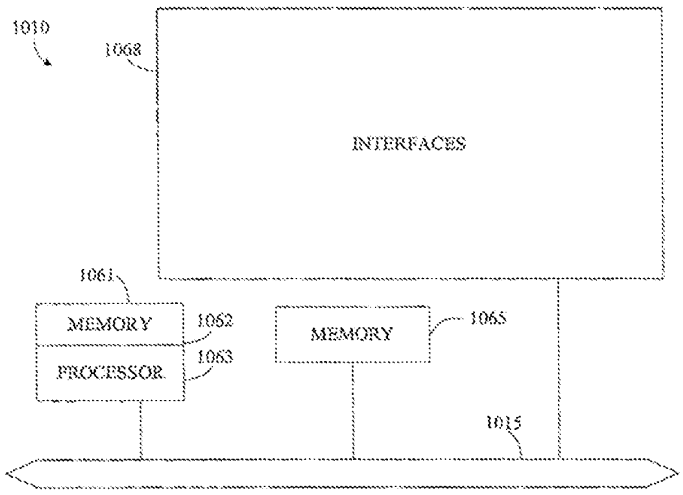
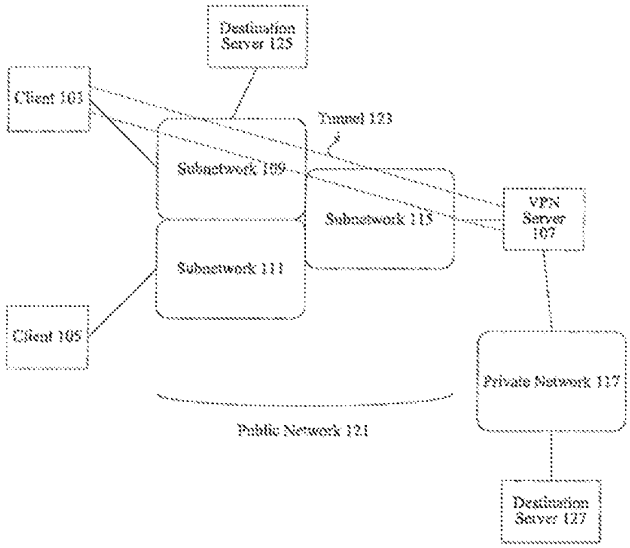


Figure 10

- Figure 10

- The public network 121 is also connected to a destination server 125 as well as clients 103 and 105. In one example, **a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 10**7. For instance, client 103 may be connected to public network 121 through an Internet service provider. In this example, client 103 may acquire a subnet work address from the Internet service provider associated with subnetwork 109. When the subnetwork address is obtained, the subnetwork address may be specifically associated with subnetwork 109. Using the subnetwork address, client 103 can access a destination server 125 in a public network 121.

	○ 4:66-5:11 ● When the subnetwork address is obtained, the subnetwork address may be specifically associated with subnetwork 109. Using the subnetwork address, client 103 can access a destination server 125 in a public network 121. However, client 103 cannot access a private network destination server 127 until it is granted access by VPN server 107. **To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107**. ○ 5:8-16
[30.2a] receive a registration request from an agent associated with a device;	*Leung* discloses *receive a registration request from an agent associated with a device* (e.g., the VPN server receives a request for access from a VPN client). ● However, client 103 cannot access a private network destination server 127 until it is granted access by VPN server 107. **To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107. In the access request, the client 103 provides information such as its subnetwork address, its user name, and its password**. ○ 5:11-18 ● In one example, **a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 107.** ○ 4:67-5:3

	Figure 1  o Fig. 1 A POSITA would have understood that *Leung*'s VPN clients would send registration requests via an associated agent. Ex. 1003, ¶49. The '785 Patent describes "communication agent[s] installed on a device" that can include "software or hardware" and "may comprise a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address." Ex. 1001 at 7:1-8. Similarly, a POSITA would have understood *Leung*'s VPN clients to include software to allow for traffic to be routed to members of the virtual community. Ex. 1003, ¶49. This software would have been required for such a client device to send an access request to the VPN server. *Id.* Thus, a POSITA would have understood that *Leung* discloses *an agent associated with a device*.
[30.2(b)] distribute a virtual network address to the device when the	*Leung* discloses *distribute a virtual network address* (e.g., enterprise address) *to the device* (e.g., VPN client) *when the device is registered in the virtual network* (e.g. private network), *the device being identified to other devices in the virtual network by the virtual network address* (e.g. the enterprise address allows the VPN server to identify a client).

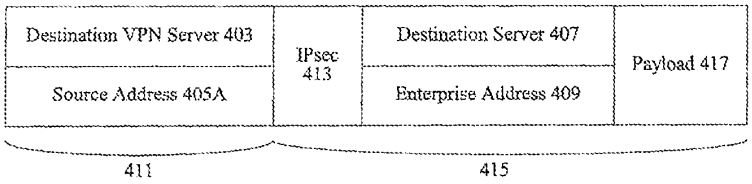
device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and	• The **client may** therefore use the client subnetwork address to **contact the VPN server** and provide the VPN server with a user name and password **to acquire an enterprise address**. **The enterprise address is the address that the VPN client uses to communicate with other nodes such as nodes in the company private network.** o 4:5-10 • **For instance, the enterprise address can be a company IP address. Thus, other nodes including nodes in the company private network will see the VPN client as having the enterprise address, and will therefore communicate with the VPN client via the enterprise address.** Accordingly, sessions between the VPN client and a node of the private network can be conducted using the enterprise address. It should be noted that a client can have two distinct addresses. An address specific to a particular subnetwork that can be obtained from an ISP is referred to herein as a subnetwork address or a client subnetwork address. The subnetwork address can be an IP address. **An address provided by a VPN server and assigned to the client is referred to herein as an enterprise address.** o 4:12-25 • To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107. In the access request, the client 103 provides information such as its subnetwork address, its user name, and its password. T**he VPN server 107 verifies the user name and password information from client 103 and provides the client 103 with an enterprise address. The enterprise address can be any address that allows a VPN server to identify a client 103.** According to various embodiments, **the enterprise address is a subnetwork address associated with the private network 117. For instance, the enterprise address may be a company IP address**. o 5:13-26 • In this example, the encapsulated portion 415, however, is typically encrypted using IPsec 413. Encapsulated portion 415 provides the VPN tunnel with security. More particularly, security is provided through enabling authentication of the sender (e.g., via information in the encapsulated portion 415) and encryption of data as well. **For instance, the encapsulated portion 415 preferably contains the enterprise address 409 allocated by the VPN server to the**

VPN client during the creation of the VPN tunnel, which may be used to authenticate the sender. The encapsulated portion 415 also contains the destination address of the server 407 that the client wishes to access. In one example, the destination server 407 may be a Web server containing a page that the client wishes to view. The encapsulated portion 415 may also contain a payload 417.

- 6:53-67

- FIG. 4A is a diagrammatic representation of a message that can be sent from a client to a destination when a VPN tunnel is used.
  - 6:41-43

Figure 4A



- Figure 4

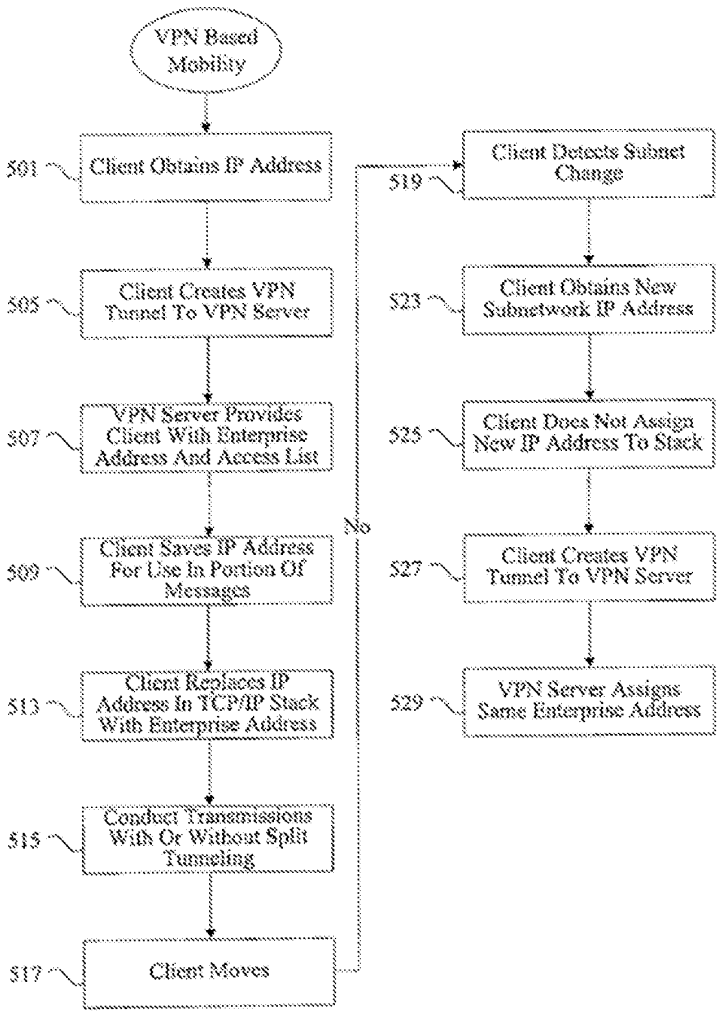
- In one implementation, a client wishes to access a Web server. A client examines the access list to determine if the Web server address is on the access list. If the Web server address is not on the access list, the client can send a packet directly to the Web server using its subnetwork address as the source address and the address of the Web server as the destination address, as shown above. If the Web server is on the access list, the client is directed to send a packet to the Web server through a VPN tunnel and a VPN server. **The client uses its own address as the source address and the address of the VPN server as the destination address of a message. The message contains an encapsulated portion 415 with a destination address 407 set as the address of the Web server and the source address 409 set as the enterprise address allocated by the VPN server. When the VPN server receives the message, the VPN server can decrypt the message, authenticate the sender via the enterprise address (source address 409) and forward the encapsulated portion 415 of the message to the web server.**

	○ 7:1-20 ● The web server receives the encapsulated portion of the message and sees that the source of the message is the enterprise address. The web server can send content to the enterprise address represented by the VPN server. **The VPN server can then encapsulate the content and forward the content to the client. As noted above, the web server does not know the actual subnetwork address of the client. The web server may only know the enterprise address**. In other words, the VPN server performs a mapping of the enterprise address to the client address. ○ 7:20-30 ● The present invention allows the maintenance of existing sessions between a client and a destination node when the client moves from a first subnetwork to a second subnetwork. According to various embodiments, existing sessions can be maintained by modifying the VPN client and the VPN server. More particularly, **the VPN client and the VPN server can be modified to allow the VPN client to use the same enterprise address whether the VPN client is in a first subnetwork or a second subnetwork. By using the same enterprise address, a client's existing sessions with a Web server, for example, can be maintained because the Web server can continue to send messages to the client using the same address.** ○ 8:1-13 ● FIG. 5 is a process flow diagram depicting some of the changes that can be made to the VPN client to allow the VPN client to seamlessly roam from a first subnetwork to a second subnetwork. **At 501, a client is in a first subnetwork and obtains a first subnetwork address from an Internet service provider. The first subnetwork address is inserted into the TCP/IP stack to allow communication with other nodes in the network. At 505, the client attempts to set up a VPN tunnel with the VPN server by transmitting the first subnetwork address, a username, and a password to the VPN server. The VPN server verifies the information and provides the client with an enterprise address as well as an access list at 507.** At 509, the client saves the first subnetwork address to use as an outer portion source address for outgoing packets. For instance, the first subnetwork address can be saved in the device driver or in the operating system. **At 513, the VPN client replaces the first subnetwork address in the TCP/IP stack with the enterprise address acquired from the VPN**

	server. By replacing the first subnetwork address with the enterprise address, the enterprise address can be used for all communications whether the client is in a first subnetwork or a second subnetwork. At 515, the client can send messages with or without the VPN tunnel. If messages are sent without the VPN tunnel, the source address is the first subnetwork address and the destination address can be the destination node of interest. If messages are sent through the VPN tunnel, the source address is the first subnetwork address and the destination address is the address of the VPN server. The encapsulated destination address is the destination node of interest and the encapsulated Source address is the enterprise address. Such a message resembles the message shown in FIG. 4A. ○ 8:14-45 ● At 517, the client moves from a first subnetwork to a second subnetwork. At 519, the client detects the change in subnetworks without user intervention. One of the benefits of the techniques of the present invention is that VPN based mobility can be accomplished in a manner transparent to the user. In many conventional applications, the client moving from a first subnetwork to a second subnetwork had to acquire a new subnetwork address and manually start the creation of a new VPN tunnel. Existing sessions would be dropped. However, the techniques of the present invention allow a VPN tunnel and existing sessions to be maintained without user interaction. The seamless mobility can be accomplished by automatically detecting a change in sub network using lower layer protocols. A variety of conventional mechanisms for detecting Subnet changes are available. Some techniques include using the lifetime field from a router advertisement using IRDP as described in RFC 1256 or using network prefixes as described in RFC 2002, the entirety of which is incorporated by references for all purposes. ○ 8:46-65 ● The VPN client can then automatically obtain a second subnetwork address associated with the second subnetwork at 523. In one embodiment, the second subnetwork address can be obtained using DHCP. In other embodiments, a second subnetwork address can be automatically entered by a VPN client. At 525, the VPN client recognizes the change in Subnetworks and does not replace the enterprise address in the TCP/IP stack with the second subnetwork address. The second subnetwork address instead can be saved in the device driver. **The enterprise address remains the same in the TCP/IP stack. Without user intervention, the VPN client**

	automatically attempts to re-establish the VPN tunnel by sending the second Subnetwork address, a username, and a password to the VPN server. The tunnel to the VPN server is created at 527. Because of modifications to the VPN server which will be discussed below, the VPN server assigns the same enterprise address to the VPN client at 529. By providing the same enterprise address to the VPN client, existing sessions are maintained. As will be appreciated by one of skill in the art, although the techniques of the present invention can be accomplished without user intervention, it will be appreciated that certain circumstances may benefit from user input. Various techniques for acquiring a new subnetwork address and establishing a VPN tunnel can also be accomplished manually. ○ 8:66-9:23

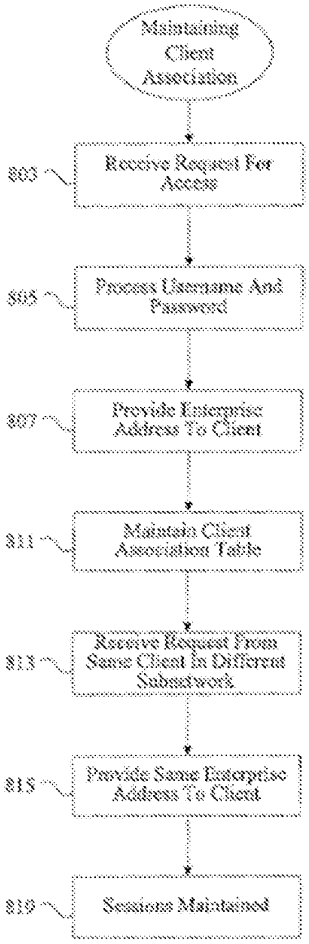
Figure 5



- Figure 5

- FIG. 8 is a process flow diagram showing modifications to the server that can be used to provide a VPN client with the same enterprise address. **At 803, the VPN server receives a request for access. The request for access may include the subnetwork address, a username, and a password of a VPN client. At 805, the VPN server verifies the username and password. At 807, the VPN server provides an enterprise address to the VPN**

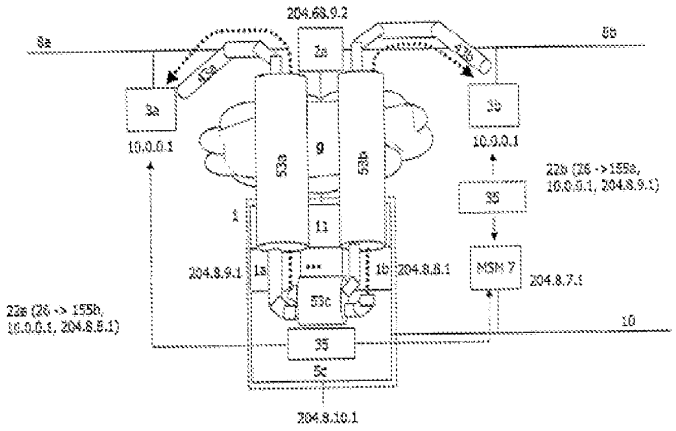
	client to allow the VPN client to establish a VPN tunnel. The VPN server maintains a client association table at 811. Any mechanism providing an association between the client and the enterprise address is referred to herein as a client association table. For instance, the client association table can be maintained in a table listing usernames and their associated enterprise addresses. The client association table can also be maintained using various databases and log files providing information on client identifiers, usernames, and enterprise addresses. **By maintaining an association between the client and the enterprise address, the VPN server can provide the same enterprise address to a client even if the client is registering from a different subnetwork address associated with a different subnetwork. If a client moves from a first subnetwork to a second subnetwork and registers with a second subnetwork address, the VPN server can recognize the client with the username.** At 813, the VPN server receives an access request having a second Subnet work address, a username, and a password of the same VPN client. The VPN server can access the client association table to determine whether the VPN client has been provided an enterprise address in the past. The VPN server can then provide the VPN client the same enterprise address. **By maintaining the association between the client and the enterprise address, the enterprise address can be provided to the same client at 815 even though the client is registering with a different subnetwork address. By maintaining the enterprise address, sessions are maintained at 819.** o 9:52-67– 10:1-21

	Figure 8  o Figure 8
[30.3] a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the	*Leung* does not expressly disclose such *a DNS server,* but the combination of *Forslöw* and *Mehta* does. ***Forslöw*** *Forslöw* discloses, or at least renders obvious, *a DNS server for the virtual network* (e.g., mobile service manager 7)*, the DNS server configured to receive a DNS request from a first device in the virtual network* (e.g., mobile service manager 7 receives HTTPS request 22a from mobile node

virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.[1]	3a), *and return a private network address associated with a second device in the virtual network* (e.g., the mobile node 3b private IP address 156b (10.0.0.1)), *and a virtual network address associated with the second device* (e.g., the virtual home agent's 1b public IP address 157b (204.8.9.1)). A POSITA would have understood that *Forslöw*'s mobile service manager 7 functions as a DNS server by receiving HTTPS requests from mobile nodes 3a and/or 3b and returning "user fully qualified domain name 155b/155a, the mobile node 3 private IP address (10.0.0.1) and the virtual home agent's la/lb public IP address (204.8.9.1 and 204.8.8.1 respectively)." Ex. 1006, 7:2-8; x. 1003, ¶52. This functionality is similar to the VCN Manager disclosed as the DNS server in the '785 Patent, which receives a DNS request and returns a response including "the public IP address for private Route Director 2204, the private IP address for member M1 and the virtual IP address for member M1," and in some embodiments, a token key. Ex. 1001, 31:24-33. • FIG. 2 shows the tunnel structure that is established in order to allow two mobile nodes 3a and 3b to be part of the same extranet workgroup in a secure manner. Note that both mobile node 3a and 3b are given the IP address 10.0.0.1 as their mobile virtual private networks have overlapping address realms. The foreign agent 2a is given a public IP address 204.68.9.2 as is the two virtual home agents 1a and 1b. Virtual home agent 1a has IP address 204.8.9.1 and virtual home agent 1 b has IP address 204.8.8.1. Equally important is that the mobile service manager 7 is given a public IP address 204.8.7.1 that is unique across both mobile virtual private network realms. ○ 9:62-10:6

[1] Based on the claim charts filed in district court litigation involving the '785 Patent, it appears that Patent Owner interprets this claim limitation to not require that the DNS server return a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device. *See, e.g.,* Ex. 1010 at 16-18. As shown here, *Leung* in view of *Forslöw* and *Mehta* renders obvious this element whether the claim is determined to require merely that those two addresses exist or that they are required to be returned by the DNS server.

Fig. 2



- Figure 2

- The home agent 1 also contains a backbone virtual router 5c that act as the common gateway towards the Internet 6 for all virtual home agents 1a and 1b. **The backbone virtual home agent 5c also hosts a management network 10 to which a mobile service manager 7 for the mobile workgroup system is attached. The mobile service manager 7 contains among other things a portal for workgroup membership list retrieval. The workgroup membership list is used in this invention to handle communication between workgroup members belonging to different address realms (mobile virtual private networks).** However, it has also a more general appeal as a member list for creating any type of conference calls within the workgroup (e.g. by using Microsoft Netmeeting)
  - 9:30-43

- **The mobile nodes 3a and 3b that are belonging to an extranet workgroup retrieve a list of workgroup members 26 by doing HTTPS requests 22a and 22 b to the mobile service manager 7 and its portal. For each workgroup participant a triplet including the user fully qualified domain name 155 b/155 a, the mobile node 3 private IP address 156 a/b (10.0.0.1) and the virtual home agent's 1 a/1 b public IP address 157 a/b (204.8.9.1 and 204.8.8.1 respectively).** The triplets are retrieved at sign-on to the extranet workgroup and can be updated regularly through a push or pull procedure from the mobile service manager 7 portal. **A network address port translator 35 in the backbone virtual**

	router 5c allows for the traversal of the HTTPS requests 22a and 22b from the mobile nodes 3a and 3b to the mobile service manager 7. o 10:7-20 • **FIG. 4a illustrates the registration procedure message flow when creating an extranet workgroup in a network-based mobile workgroup system, i.e. a workgroup with participants from more than one mobile virtual private network**. The virtual home agents 1a and 1b are using the lightweight directory access protocol (LDAP) 25 to retrieve the extranet workgroup configurations. **The virtual home agent 1a sends an LDAP request 25a to the mobile service manager 7. The mobile service manager 7 replies with an LDAP answer 25b including any static routes 63 and filter states 64 to be applied to the workgroup traffic.** o 10:54-64 • The mobile nodes 3a and 3b within the extranet workgroup asks for the workgroup member list 26 as part of a HTTPS request 22 a/22 b. **The mobile service manager 7 responds with giving the triplets (the user fully qualified domain name 155 and private IP address 156 of the mobile node 3 as well as its virtual home agent 1 public IP address 157) for each workgroup member. This means that mobile node 3a receives the triplets for mobile node 3b and vice versa.** o 11:9-17 • **As in the normal mobile IP registration procedure, the mobile node 3a sends a registration request 46a with only its MAC address 51a as source and its virtual home agent 1a as destination to the foreign agent 2a. The foreign agent 2a forwards the registration request 46b further to the virtual home agent 1a. The registration reply 47a is sent from the virtual home agent 1a to the foreign agent 2a and forwarded to the mobile node 3a in the form of registration reply 47b**. The next sequence shows the corresponding procedure for mobile node 3b. Note that both mobile nodes are capable of using the same foreign agent 2a. o 11:18-28 • The center module of a virtual home agent 1a/b is the virtual router 5 a/b. **The virtual router is making nexthop decisions for datagrams passing through the virtual home agent 1 a/b**. It is realm-specific to the mobile virtual private network that the virtual home agent 1a/b belongs to, and in such away can only route packets

	that either has public destination IP addresses or private IP addresses that belong to the address realm of its mobile virtual private network. o 12:14-21 • The mobile service manager (MSM) 7 for a company will typically be placed at the WAN distribution layer 36 in order to be accessible from the inside as well as from the outside. **From a network perspective it will function as a centralized data store from which the mobility routers 31 can fetch user and workgroup profiles. From a management viewpoint, it will be the portal to which the IT-administrator and workgroup members login for managing profiles and exchanging service information**. o 15:57-65 ***Mehta*** While *Forslöw* discloses *a route director* (e.g., router dispatcher 11), it does not explicitly disclose that the DNS server for the virtual network *returns a network address associated with the network route director*. To the extent it is determined that additional disclose is necessary, *Mehta* discloses, or at least renders obvious *a DNS server for the virtual network* (e.g., a DNS'/API server of the Address Management Proxy System), *the DNS server configured to receive a DNS request from a first device in the virtual network* (e.g., DNS'/API server receives a request from a device on a public network), *and return a network address associated with a network route director* (e.g., the DNS'/API server returns the determined public network address of the associated Address Proxy /Router machine). The address of the proxy/router machine returned in Mehta is a public address. Similarly, in the '785 Patent the network address associated with the network route director is a public address. *See, e.g.,* Ex. 1001, 14:23-46. Furthermore, to the extent it is determined that *Forslöw*'s mobile service manager is not a DNS server, it would have been obvious to a POSITA to implement it as a DNS server, as disclosed in *Mehta*, with the functionality to return the same addresses in the triplet disclosed in *Forslöw*, as well as the public IP address for the route director, as disclosed in *Mehta*. *See* Ex. 1003, ¶52. • In one embodiment, the AMPS comprises one or more modified **DNS/API servers, one or more Address Proxy/Routers, an Address Management Data Server,** one or more Address Management Data Repositories, and optionally a load balancer**. The AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device, and**

	returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device. The public address is then usable by the device on the external public network to send data to the wireless device. The temporary public address is, for example, an address associated with one of the Address Proxy/Routers, which are connected to the external public network and have access to the private addresses on the private wireless network. In some cases, the device on the public network that desires to send data to the wireless device uses a connection-based protocol, such as TCP/IP to send data. In other cases the device uses a connection-less protocol, such as UDP (UDP/IP) to send the data. ○ [0012] ● In operation, **when a wired device such as wired device 201, desires to send data to wireless device 240, the wired device needs first to determine a routable address location of the wireless device 240 on the public network 210**. However, as can be observed from FIG. 2, the wireless device 240 is not directly connected to the public network 210. Thus, the wired device must use the Address Management Proxy System 220 to determine a routable (public) address to which to send the data destined for the wireless device 240. **To accomplish this task, the wired device 201 performs a query (for example, a modified DNS query) to locate a routable public address that corresponds to wireless device 240. The Address Management Proxy System 220 receives the query and determines and assigns a public (routable) address from a pool of addresses, which address can be used as a destination address for data packets targeted to wireless device 240.** One should note that, although shown here as a DNS query, the Address Management Proxy System, as will be described further, modifies the DNS query implementation to handle wireless device technology, and/or provides an alternative API for determining a suitable routable address. **Once the Address Management Proxy System 220 has returned a routable address to wired device 201, the wired device 201 can send data to that address**. ○ [0031] ● FIG. 3 is an example block diagram of components of an example Address Management Proxy System. In one embodiment, the Address Management Proxy System (AMPS) comprises one or more modified DNS'/API servers 302, one or more Address Proxy/Routers 305, an Address Management Data Server 303 which manages a database or other repositories such as Address Management Data Repository 304, and optionally a load balancer

	301. **The DNS'/API servers 302 are either individually connected to a public network 310 or are connected to the load balancer 301 which is in turn connected to public network 310**. **Similarly, each Address Proxy/Router 305 is also connected to the public network 310, via the routable (public) address to which data from the external network 310 is sent that is destined for the wireless devices.** The DNS'/API servers 302 are either modified implementations of a DNS server to add functionality necessary to communicate with wireless devices, or are servers that implement one or more specialized APIs, as will be described further below. The DNS'/API servers 302 use the Address Management Data Server 303 to assist in mapping a unique identifier (e.g., string name) for a wireless device to a public address on public network 310. The pool of public addresses is also maintained by the Address Management Data Serve 303 and Data Repository 304. The Address Management Data server 303 and Address Management Data Repository 304 may be implemented using existing database technology, for example, ODBC technology or, may be implemented as a structure such as a simple text file. One skilled in the art will recognize that any embodiment for storing a set of tables, data, lists, or map pings can be used. **Each Address Proxy/Router 305 also uses the Address Management Data Server 303 or equivalent to create and update a series of routing tables that are used to assign public addresses to wireless devices as needed and to update the various mappings between public addresses and the non-routable (private) addresses of the wireless devices**. The tables and mappings that are maintained on behalf of the DNS'/API servers 302 and the Address Proxy/Routers 305 by the Address Management Data Server 303 are described below with reference to FIG. 6. ○ [0032] ● FIG. 7 is an example flow diagram of an example routine provided by a DNS'/API server of the Address Management Proxy System to return a public address that corresponds to a designated unique identifier. In essence, this routine implements a DNS query or DNS-like query capability for the AMPS using a modified GetHostByName interface or a specialized API, for example GetProxyIP, as described with reference to FIG. 5. **In summary, the routine dynamically allocates an appropriate Address Proxy/Router machine to associate with the wireless device and returns the public address of that machine (along with a TTL parameter and potentially other parameters)**. Specifically, in step 701, the routine determines the private (non-routable) address of the wireless device designated by a string parameter passed as input to

	the routine. For example, the string parameter may use fields such as "uniqueID.hostname.domain.tld," which specifies a typical hierarchy of person/service on a machine named "hostname" on a domain such as a company's network on a top level domain such as "org.""com, ""edu," etc. One skilled in the art will recognize that many other string parameter designations could be used. One mechanism for implementing this routine is to request information from the Address Management Data Repository. In one embodiment, the data repository stores a table that maps unique IDs to private network addresses (see Table 610 in FIG. 6). Preferably, any mechanism that is used by the AMPS stores this data in a secure manner in order to keep the wireless network addresses private. **In step 702, the routine retrieves the public network address that corresponds to the private wireless network address of the designated device if one has already been assigned by the AMPS to that device and is still valid. In one embodiment, the data repository stores this mapping information between private wireless network address and public network address (see for example table 630 in FIG. 6).** If a public network address has not already been assigned or is not valid, then the routine causes a new public network address to be allocated and that new public address is associated with the private wireless network address. Appropriate tables in the data repository are then updated. **In step 703, the routine determines the Address Proxy/Router machine that is associated with the assigned public network address (for example using table 620 in FIG. 6). In step 704, the routine sends a request to the determined proxy/router machine to update its routing tables to map the determined public network address to the private wireless network address.** In step 705, the routine updates information in the data repository to include any other connection related information (e.g., field 634 in Table 630 in FIG. 6) and indicates a Time to Live (TTL) parameter for the public-private address association (e.g., field 633 in Table 630 in FIG. 6). **Once all of the tables have been updated in both the proxy/router and in the data repository, the DNS'/API server returns the determined public network address of the associated Address Proxy /Router machine**. As described earlier, the public address may be a (hostname, port) pair when a port-based implementation is used. ○ [0057]

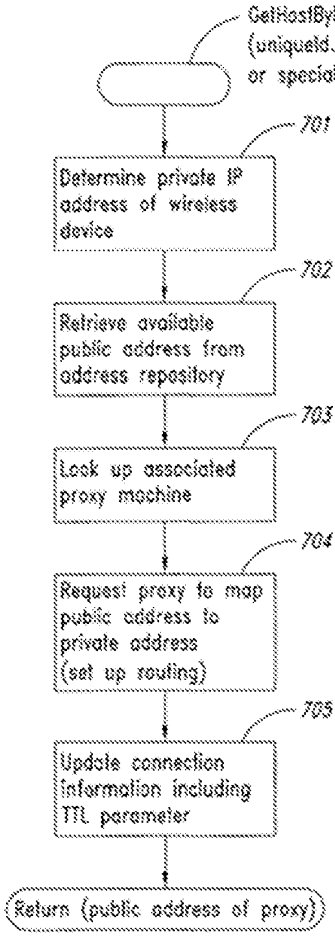


Fig. 7

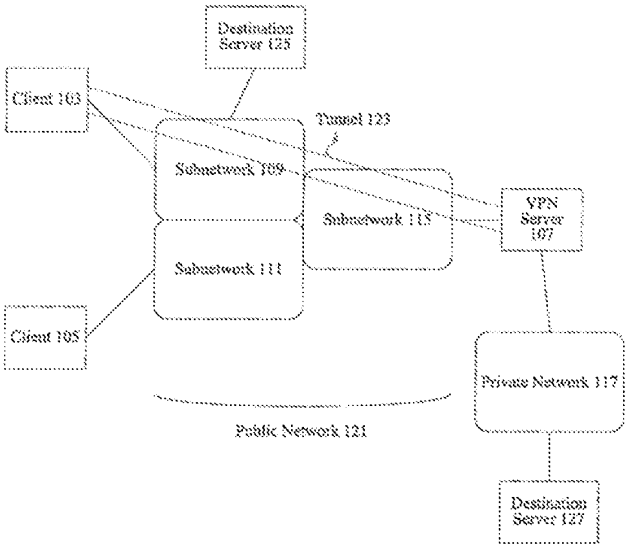
- Fig. 7

- FIG. 8 is an example flow diagram of an example routine within an Address Proxy/Router of an example Address Management Proxy System that receives data. This routine is implemented by an Address Proxy/Router to receive data from wired devices using the relevant protocol (e.g., TCP/IP, UDP/IP, etc.). (**Data is sent to a**

	particular Address Proxy/Router because the public (routable) address of that Address Proxy /Router was returned to the requesting/ source device in response to a query of the DNS'/API server of the AMPS.) The proxy/router is responsible for any conversions of the data necessary to send data from the wired network to the wireless network (if, for example, the carrier infrastructure desires such conversion to be performed at this level). **The proxy /router is also responsible for forwarding the data via the wireless network to the private wireless address of the wireless device that corresponds to the public address used to invoke the proxy/router.** ○ [0058] **Motivations to Combine Leung, Forslöw, and Mehta** It would have been obvious to a POSITA to incorporate *Forslöw*'s and *Mehta*'s teachings related to a communication across virtual networks into *Leung*'s virtual private network system. Ex. 1003, ¶¶56-61. *Leung* discloses a VPN system in which client devices gain access to the VPN in order to send data to devices within the VPN. *See, e.g.*, Ex. 1005, 5:8-18. *Forslöw* discloses a similar VPN, but specifically details the way in which the DNS server (which it calls a mobile service manager) facilitates communication over the VPN system. *See, e.g.,* Ex. 1006, 9:62-10:20. A POSITA would have been motivated to make such a combination because implementation of *Forslöw*'s VPN tunnelling system would have allowed data messaging to be sent in a more efficient and secure manner. Ex. 1003, ¶56. Additionally, *Forslöw*'s VPN system provides for a virtual route director to assist in data mapping. *See, e.g.,* Ex. 1006, 9:19-29. *Mehta* discloses a similar virtual networking system that operates with a DNS server and a route director, but it goes into more details about the operation of the route director, and thus provides for such DNS servers to provide private to network address associated with a network address proxy machine. *See, e.g.,* Ex. 1007, [0012], [0031]-[0032]. A POSITA would have been motivated to make this combination because implantation of *Mehta*'s utilization of the DNS server would have aided in the security of the VPN system created by the combination of *Leung* and *Forslöw*. Ex. 1003, ¶57. Furthermore, a POSITA would have been motivated to combine *Leung*, *Forslöw*, and *Mehta* because the combination merely uses a known technique to improve similar devices in the same way. See *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 401 (2007). For instance, the combination would have merely required the use of a known technique, specifically the utilization of routing via addresses provided by a DNS server to similar VPN systems in the same way. Ex. 1003, ¶58 (*citing* Ex.

	1008 (Kong), 2:15-42, 5:17-6:5 and Ex. 1009 (Volz) at 5:13-26, 11:31-64, 19:47-20:15). A POSITA would have had a reasonable expectation of success in modifying *Leung*'s VPN system, which allows for registration and data transmission by client devices, to perform this data transmission via use of a DNS server and route director, as taught by *Forslöw* and *Mehta*, because doing so would merely have implemented a well-known technique in the VPN system of *Leung*, as shown above. Ex. 1003, ¶59. Therefore, a POSITA would have been motivated to combine, and would have had a reasonable expectation of success in combining *Forslöw*'s and *Mehta*'s teachings related to the use of a DNS server in a virtual network system with *Leung*'s teaching related to a VPN system. Ex. 1003, ¶¶56-61. Thus, *Leung*, in combination with *Forslöw* and *Mehta*, teaches this limitation.
Claim 34	
[34.0] The virtual network manager of claim 30 wherein	*See mapping of claim 30 above.*
the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network.	*See mapping of elements [30.2] and [30.3], above, for how Leung discloses a register module that is configured to receive a registration request from an agent associated with a device.* *Leung* discloses *the register module* (e.g., software on CPU 1062) *is further configured to receive the registration request* (e.g., access request) *from the agent that is installed on the device* (e.g., software on the VPN client) *for data communication via the virtual network* (e.g., sending a data packet via the VPN). ● However, client 103 cannot access a private network destination server 127 until it is granted access by VPN server 107. **To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107. In the access request, the client 103 provides information such as its subnetwork address, its user name, and its password**. o 5:11-18 ● In one example, **a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 107.** o 4:67-5:3

Figure 1

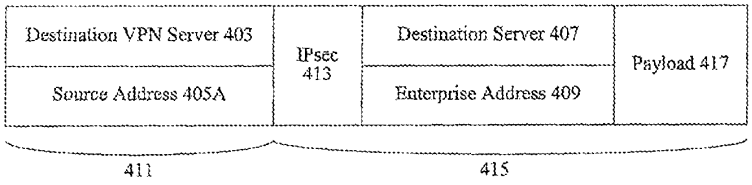


- Fig. 1

- In this example, the encapsulated portion 415, however, is typically encrypted using IPsec 413. Encapsulated portion 415 provides the VPN tunnel with security. More particularly, security is provided through enabling authentication of the sender (e.g., via information in the encapsulated portion 415) and encryption of data as well. **For instance, the encapsulated portion 415 preferably contains the enterprise address 409 allocated by the VPN server to the VPN client during the creation of the VPN tunnel, which may be used to authenticate the sender.** The encapsulated portion 415 also contains the destination address of the server 407 that the client wishes to access. In one example, the destination server 407 may be a Web server containing a page that the client wishes to view. The encapsulated portion 415 may also contain a payload 417.
  - 6:53-67

- FIG. 4A is a diagrammatic representation of a message that can be sent from a client to a destination when a VPN tunnel is used.
  - 6:41-43

Figure 4A



  - Figure 4

A POSITA would have understood that *Leung*'s VPN clients would send registration requests via an associated agent. Ex. 1003, ¶49. The '785 Patent describes "communication agent[s] installed on a device" that can include "software or hardware" and "may comprise a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address." Ex. 1001 at 7:1-8. Similarly, a POSITA would have understood *Leung*'s VPN clients to include software to allow for traffic to be routed to members of the virtual community. Ex. 1003, ¶49. This software would have been required for such a client device to send an access request to the VPN server. *Id.* Thus, a POSITA would have understood that *Leung* discloses *an agent associated with a device*.

EXHIBIT 1001
U.S. Patent 7,949,785 to Alkhatib
(the "*'785 Patent*")

US007949785B2

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

(10) **Patent No.: US 7,949,785 B2**
(45) **Date of Patent: May 24, 2011**

(54) **SECURE VIRTUAL COMMUNITY NETWORK SYSTEM**

(75) Inventors: **Hasan S. Alkhatib**, Saratoga, CA (US); **Fouad A. Tobagi**, Los Altos, CA (US); **Farid F. Elwailly**, San Jose, CA (US)

(73) Assignee: **Inpro Network Facility, LLC**, Wilmington, DE (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 685 days.

(21) Appl. No.: **10/403,818**

(22) Filed: **Mar. 31, 2003**

(65) **Prior Publication Data**

US 2004/0249911 A1 Dec. 9, 2004

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/245**; 726/15

(58) **Field of Classification Search** 709/245; 726/15

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A	10/1992	Perkins	
5,361,256	A	11/1994	Doeringer	
5,563,878	A	10/1996	Blakeley	
5,623,605	A	4/1997	Keshav	
5,701,427	A	12/1997	Lathrop	
5,717,686	A	2/1998	Schiavoni	
5,717,687	A	2/1998	Minot	
5,734,651	A	3/1998	Blakeley	
5,751,961	A	5/1998	Smyk	
5,754,938	A *	5/1998	Herz et al.	725/116
5,764,906	A	6/1998	Edelstein	
5,777,989	A	7/1998	McGarvey	
5,781,550	A	7/1998	Templin	
5,790,548	A	8/1998	Sistanizadeh	
5,793,763	A	8/1998	Mayes	
5,805,818	A	9/1998	Perlman	
5,805,820	A	9/1998	Bellovin	
5,815,664	A	9/1998	Asano	
5,826,014	A	10/1998	Coley	
5,856,974	A	1/1999	Gervais	
5,864,666	A	1/1999	Shrader	
5,867,667	A	2/1999	Butman	
5,884,038	A	3/1999	Kapoor	

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 817 444 A2 1/1998

OTHER PUBLICATIONS

Venters, Demystifying Protocols: A comparison of Protocols Suitable for IP Telephony, Sonus Networks, pp. 1-11, 2000.

(Continued)

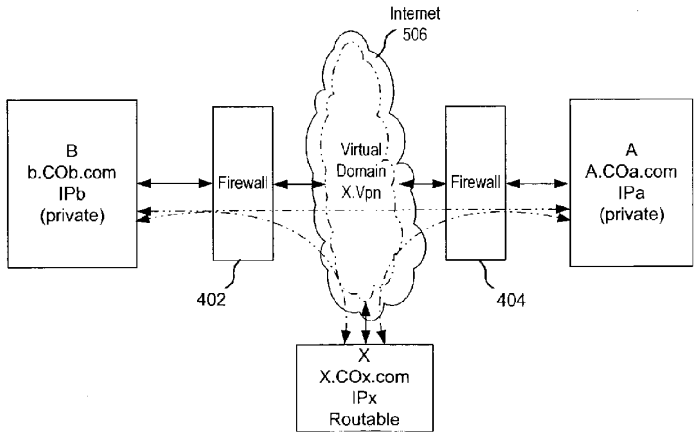
Primary Examiner — Donglas B Blair

(74) *Attorney, Agent, or Firm* — McAndrews, Held & Malloy, Ltd.

(57) **ABSTRACT**

A private virtual dynamic network is provided for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. In one embodiment, the present invention provides a separate private virtual address realm, seen to each user as a private network, while seamlessly crossing public and private network boundaries. One implementation of the present invention uses an agent to enable an entity to participate in the network without requiring the member to add new hardware or software.

90 Claims, 21 Drawing Sheets



U.S. PATENT DOCUMENTS

5,884,246	A	3/1999	Boucher	
5,889,953	A	3/1999	Thebaut	
5,897,662	A	4/1999	Corrigan	
5,898,830	A	4/1999	Wesinger, Jr.	
5,913,210	A	6/1999	Call	
5,937,162	A	8/1999	Funk	
5,937,163	A	8/1999	Lee	
6,003,084	A	12/1999	Green	
6,006,272	A	12/1999	Aravamudan	
6,032,196	A	2/2000	Monier	
6,047,325	A	4/2000	Jain	
6,055,236	A	4/2000	Nessett	
6,055,575	A	4/2000	Paulsen	
6,058,431	A	5/2000	Srisuresh	
6,061,349	A	5/2000	Coile	
6,061,738	A	5/2000	Osaku	
6,101,543	A	8/2000	Alden	
6,119,171	A	9/2000	Alkhatib	
6,122,276	A	9/2000	Boc	
6,128,664	A	10/2000	Yanagidate	
6,137,791	A	10/2000	Frid	
6,154,777	A	11/2000	Ebrahim	
6,154,839	A	11/2000	Arrow	
6,173,399	B1	1/2001	Gilbrech	
6,219,715	B1	4/2001	Ohno	
6,226,751	B1 *	5/2001	Arrow et al.	726/15
6,243,749	B1	6/2001	Sitaraman	
6,249,801	B1	6/2001	Zisapel	
6,266,707	B1	7/2001	Boden et al.	
6,304,906	B1	10/2001	Bhatti	
6,353,614	B1	3/2002	Borella	
6,353,886	B1	3/2002	Howard	
6,381,638	B1	4/2002	Mahler	
6,421,732	B1	7/2002	Alkhatib	
6,430,622	B1	8/2002	Aiken, Jr.	
6,430,623	B1	8/2002	Alkhatib	
6,438,597	B1	8/2002	Mosberger	
6,438,612	B1	8/2002	Ylonen	
6,452,925	B1	9/2002	Sistanizadeh	
6,457,061	B1	9/2002	Bal	
6,477,565	B1	11/2002	Daswani et al.	
6,480,508	B1	11/2002	Mwikalo	
6,490,289	B1	12/2002	Zhang et al.	
6,496,867	B1	12/2002	Beser	
6,507,873	B1	1/2003	Suzuki	
6,510,154	B1	1/2003	Mayers	
6,523,068	B1	2/2003	Beser	
6,556,584	B1	4/2003	Horsley	
6,557,037	B1	4/2003	Provino	
6,557,306	B1	5/2003	Sekiya	
6,591,306	B1	7/2003	Redlich	
6,594,704	B1 *	7/2003	Birenback et al.	709/238
6,618,757	B1	9/2003	Babbitt	
6,629,137	B1	9/2003	Wynn	
6,631,416	B2 *	10/2003	Bendinelli et al.	709/227
6,651,101	B1	11/2003	Gai	
6,657,991	B1	12/2003	Akgun	
6,662,223	B1	12/2003	Zhang	
6,697,377	B1	2/2004	Ju	
6,701,437	B1 *	3/2004	Hoke et al.	726/15
6,708,219	B1	3/2004	Borella et al.	
6,722,210	B2	4/2004	Armstrong	
6,731,642	B1	5/2004	Borella	
6,742,045	B1	5/2004	Jordan	
6,747,979	B1	6/2004	Banks	
6,754,706	B1	6/2004	Swildens	
6,772,210	B1	8/2004	Edholm	
6,778,528	B1	8/2004	Blair	
6,779,035	B1	8/2004	Gbadegesin	
6,781,982	B1	8/2004	Borella	
6,832,322	B1 *	12/2004	Boden et al.	726/15
6,948,003	B1	9/2005	Newman	
6,961,783	B1 *	11/2005	Cook et al.	709/245
6,970,941	B1 *	11/2005	Caronni et al.	709/238
6,973,485	B2	12/2005	Ebata	
6,981,020	B2	12/2005	Miloslavsky	
6,982,953	B1	1/2006	Swales	
6,983,319	B1	1/2006	Lu	
6,993,012	B2	1/2006	Liu	
6,993,595	B1	1/2006	Luptowski	
6,996,628	B2	2/2006	Keane	
6,996,631	B1	2/2006	Aiken	
7,003,481	B2	2/2006	Banka	
7,010,702	B1 *	3/2006	Bots et al.	726/13
7,028,333	B2	4/2006	Tuomenoksa et al.	
7,028,334	B2	4/2006	Tuomenoksa et al.	
7,032,242	B1	4/2006	Grabelsky	
7,054,322	B2	5/2006	D'Annunzio	
7,058,052	B2	6/2006	Westphal	
7,068,655	B2	6/2006	March et al.	
7,072,337	B1	7/2006	Arutyunov et al.	
7,072,935	B2	7/2006	Kehoe et al.	
7,085,854	B2	8/2006	Keane et al.	
7,092,390	B2 *	8/2006	Wan	370/392
7,107,464	B2 *	9/2006	Shapira et al.	709/200
7,107,614	B1 *	9/2006	Boden et al.	726/15
7,110,375	B2	9/2006	Khalil et al.	
7,120,676	B2	10/2006	Nelson et al.	
7,133,368	B2	11/2006	Zhang et al.	
7,139,828	B2	11/2006	Alkhatib	
7,181,542	B2 *	2/2007	Tuomenoksa et al.	709/250
7,194,553	B2 *	3/2007	Lucco et al.	709/245
7,227,864	B2	6/2007	Collins et al.	
7,263,719	B2 *	8/2007	Jemes et al.	726/12
7,327,721	B2 *	2/2008	Balasaygun et al.	370/352
7,424,737	B2 *	9/2008	Wesinger et al.	726/11
7,490,151	B2 *	2/2009	Munger et al.	709/225
7,653,747	B2 *	1/2010	Lucco et al.	709/245
7,787,428	B2 *	8/2010	Furukawa et al.	370/338
7,814,228	B2 *	10/2010	Caronni et al.	709/245
7,827,304	B2 *	11/2010	Park et al.	709/238
7,844,718	B2 *	11/2010	Polcha et al.	709/229
7,853,714	B1 *	12/2010	Moberg et al.	709/238
2001/0027474	A1	10/2001	Nachman et al.	
2001/0050914	A1 *	12/2001	Akahane et al.	370/382
2002/0013848	A1 *	1/2002	Rene Salle	709/226
2002/0026525	A1	2/2002	Armitage	
2002/0053031	A1 *	5/2002	Bendinelli et al.	713/201
2002/0056008	A1 *	5/2002	Keane et al.	709/245
2002/0078198	A1	6/2002	Buchbinder et al.	
2002/0091859	A1 *	7/2002	Tuomenoksa et al.	709/245
2002/0099937	A1 *	7/2002	Tuomenoksa	713/153
2002/0103931	A1 *	8/2002	Mott	709/245
2002/0133534	A1 *	9/2002	Forslow	709/200
2003/0018912	A1	1/2003	Boyle et al.	
2003/0041091	A1 *	2/2003	Cheline et al.	709/200
2003/0041136	A1 *	2/2003	Cheline et al.	709/223
2003/0055978	A1	3/2003	Collins	
2003/0065785	A1	4/2003	Jain	
2003/0074472	A1 *	4/2003	Lucco et al.	709/245
2003/0084162	A1	5/2003	Johnson et al.	
2003/0123421	A1	7/2003	Feige	
2003/0131131	A1 *	7/2003	Yamada et al.	709/238
2003/0152068	A1 *	8/2003	Balasaygun et al.	370/356
2003/0208554	A1	11/2003	Holder	
2003/0212795	A1	11/2003	Harris et al.	
2003/0219000	A1	11/2003	Magret	
2004/0006708	A1 *	1/2004	Mukherjee et al.	713/201
2004/0088542	A1 *	5/2004	Daude et al.	713/156
2004/0111612	A1 *	6/2004	Choi et al.	713/163
2004/0148439	A1 *	7/2004	Harvey et al.	709/249
2006/0190607	A1 *	8/2006	Lowery et al.	709/226
2006/0195524	A1 *	8/2006	Nichols et al.	709/204
2006/0195539	A1 *	8/2006	Nichols et al.	709/206
2006/0212545	A1 *	9/2006	Nichols et al.	709/219
2006/0212599	A1 *	9/2006	Lucco et al.	709/245
2007/0286189	A1 *	12/2007	Kreiner et al.	370/389
2008/0232295	A1 *	9/2008	Kreiner et al.	370/313
2009/0116487	A1 *	5/2009	Read	370/392

OTHER PUBLICATIONS

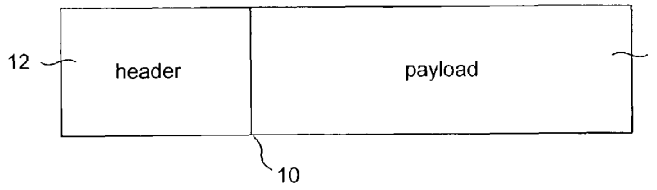
Tsuchiya, et al., Extending the IP Internet Through Address Reuse, ACM SIGCOMM Computer Communication Review, pp. 16-33, Jan. 1993.

Francis, et al., IPNL: A NAT-Extended Internet Architecture, SIGCOMM'01, Aug. 27-31, 2001, pp. 69-79.

Yalagandula, et al., Transparent Mobility with Minimal Infrastructure, University of Texas at Austin, pp. 1-14, Jul. 2001.
Teraoka, et al., VIP: A Protocol Providing Host Mobility, Communications of the ACM, Aug. 1994/vol. 37, No. 8, pp. 67-75, 113.
Egevang, et al., The IP Network Address Translator (NAT), Network Working Group, RFC 1631, May 1994, pp. 1-10.
Chatel, Classical Versus Transparent IP Proxies, Network Working Group, RFC 1919, Mar. 1996, pp. 1-35.
Finseth, An Access Control Protocol, Sometimes Called TACACS, Network Working Group, Jul. 1993, pp. 1-18.
Computer Nelowrks. Third Edition, by Andrew S. Tanenbaum, 1996, pp. 643-670, 685-691.
Perkins, Mobile IP, IEEE Communications Magazine, May 1997, pp. 84-99.
"Non-Final Office Action", U.S. Appl. No. 10/233,288, (Dec. 21, 2009), 13 pages.
"Final Office Action", U.S. Appl. No. 10/403,518, (Feb. 2, 2010), 26 pages.
"Final Office Action", U.S. Appl. No. 10/403,829, (Feb. 23, 2010), 15 pages.
"Advisory Action", U.S. Appl. No. 10/403,829, (May 14, 2010), 2 pages.
"Non Final Office Action", U.S. Appl. No. 10/161,573, (May 26, 2009),39 pages.
"Non Final Office Action", U.S. Appl. No. 10/403,829, (Jun. 22, 2009),26 pages.
Francis, Gummadi "IPNL: A NAT-Extended Internet Architecture", *SIGCOMM '01*, (Aug. 2001),69-79.
"Final Office Action", U.S. Appl. No. 10/161,573, (Jul. 23, 2010), 21 pages.
"Final Office Action", U.S. Appl. No. 10/233,288, (Aug. 3, 2010), 15 pages.
"Non Final Office Action", U.S. Appl. No. 10/403,518, (Aug. 3, 2010), 30 pages.
"Advisory Action", U.S. Appl. No. 10/233,288, (Oct. 15, 2010), 3 pages.
Tanenbaum, Andrew S., "Computer Networks", Third Edition,(1996),1-37.
Chatel, M "Classical versus Transparent IP Proxies", *Network Working Group Request for Comments*, (Mar. 1996),1-35.
Finseth, C "An Access Control Protocol , Sometimes Called TACACS", *Network Working Group Request for Comments*, (Jul. 1993),1-18.
Francis, Paul et al., "IPNL: A NAT-Extended Internet Architecture", *SIGCOMM'01*, (Aug. 1, 2008),69-79.
Perkins, Charles E., "Mobile IP", *IEEE Communications Magazine*, Sun Microsystems,(May 1997),84-99.
Teraoka, Fumio et al., "VIP: A Protocol Providing Host Mobility", *Communications of the ACM*, vol. 37, No. 8,(Aug. 1994),67-75, 113.
Tsuchiya, Paul F., et al., "Extending the IP Internet Through Address Reuse", *ACM SIGCOMM Computer Communication Review*, (January 1993),16-33.
Venters, Tracy "Demystifying Protocols: A Comparison of Protocols Suitable for IP Telephony", *Sonus Networks*, (2000),1-11.
Yalagandula, Praveen et al., "Transparent Mobility with Minimal Infrastucture", *University of Texas at Austin*, (Jul. 2001),1-14.
Kessler, Gary C., "Mobile IP: Harbiner of Untethered Computing," http://www.garykessler.net/librarymobileip.htm, Jan. 20, 2004.
Rekhter, "Cisco Systems' Tag Switching Architecture overview," Network Working Group, Feb. 1997.
Kent, "Security Architecture for the Internet Protocol," Network Working Group, Nov. 1998.
Computer Dictionary; Microsoft Press; 3rd Edition; 1997; p. 264.
K. Egevang and P. Francis, RFC 1631, The IP Network Address Translator (NAT), May 1994.
"Non Final Office Action", U.S. Appl. No. 10/403,829, (Nov. 19, 2010),19 pages.

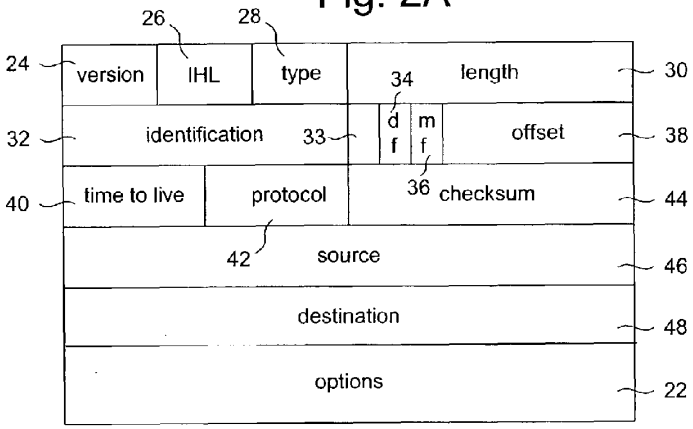
* cited by examiner

Fig. 1



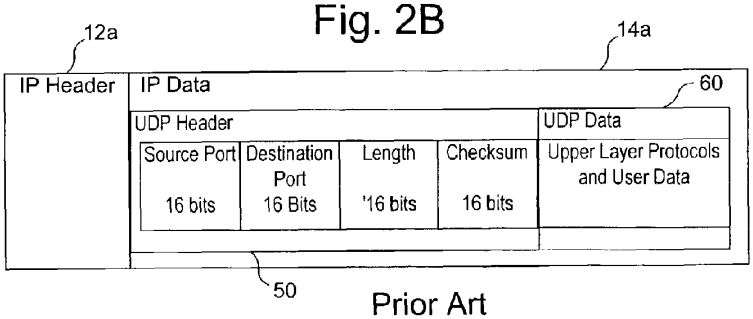
Prior Art

Fig. 2A



Prior Art

Fig. 2B



Prior Art

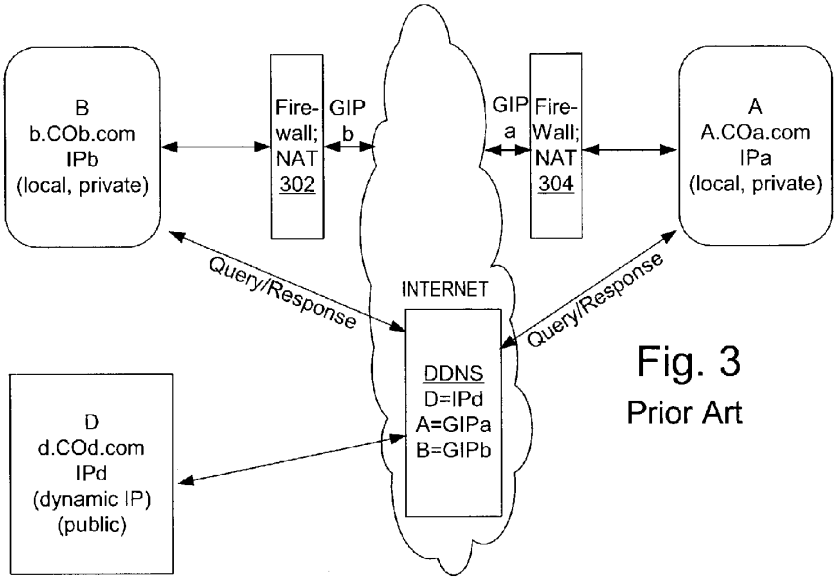


Fig. 3
Prior Art

Fig. 4

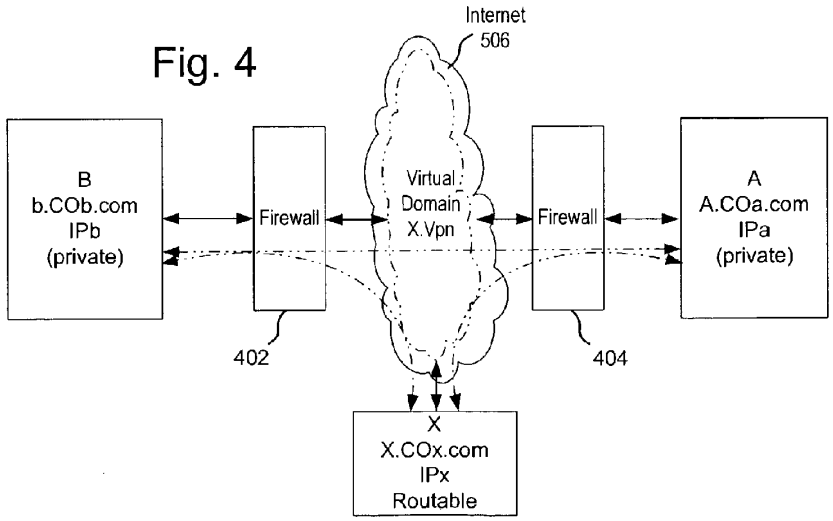
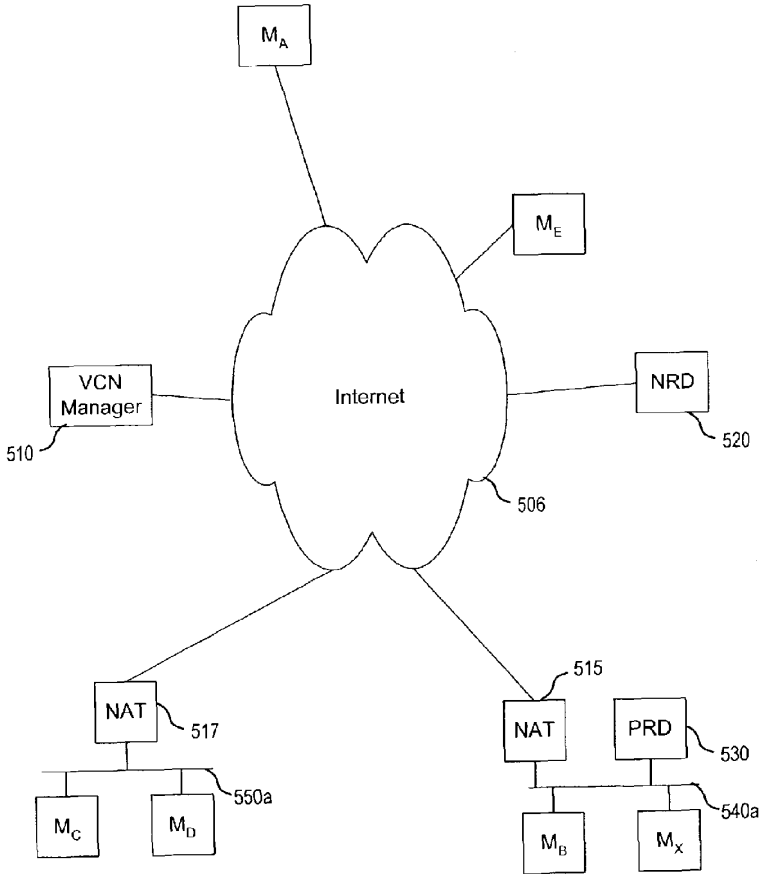


Fig. 5a


M_A
M_E
VCN Manager
510
Internet
506
NRD
520
515
NAT
517
NAT
PRD
530
550a
540a
M_C
M_D
M_B
M_X

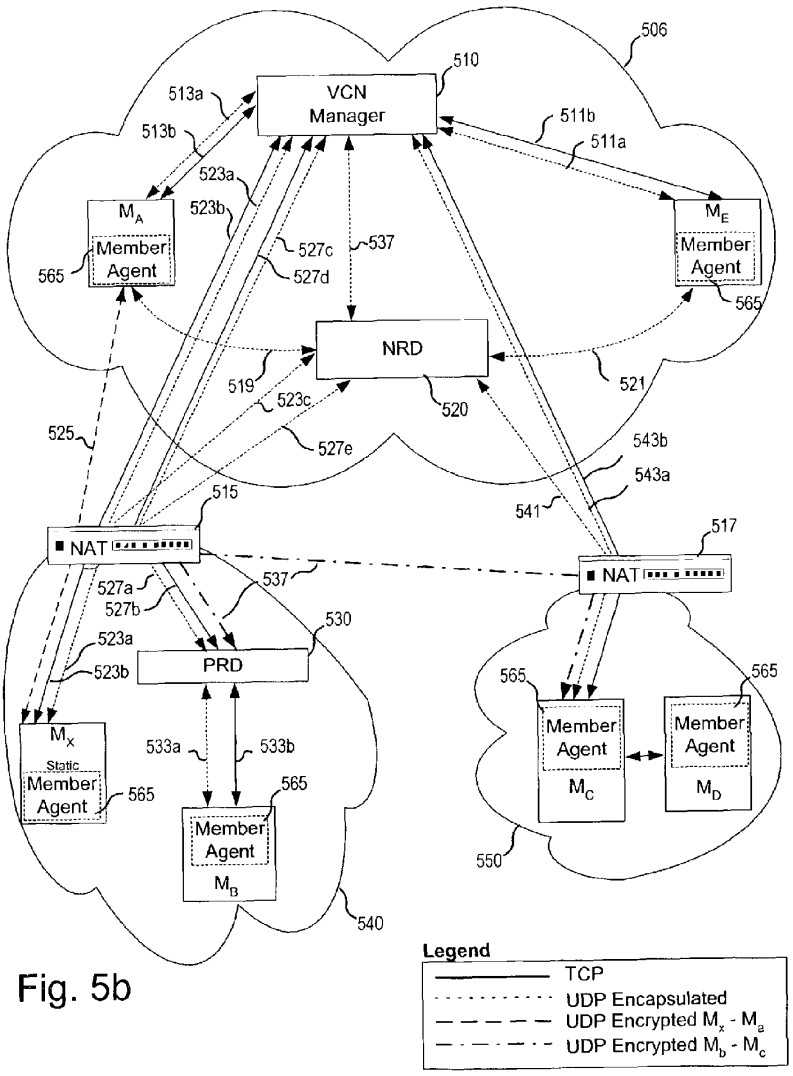

506
510
VCN Manager
513a
513b
511b
511a
523a
523b
M_A
Member Agent
565
527c
527d
537
M_E
Member Agent
565
NRD
519
523c
520
521
525
527e
543b
543a
541
515
NAT
517
NAT
527a
527b
537
530
523a
523b
PRD
565
565
M_X
Static
Member Agent
565
533a
533b
Member Agent
M_C
Member Agent
M_D
565
Member Agent
M_B
550
540
Legend
TCP
UDP Encapsulated
UDP Encrypted M_x - M_a
UDP Encrypted M_b - M_c

Fig. 5b

Fig. 6A

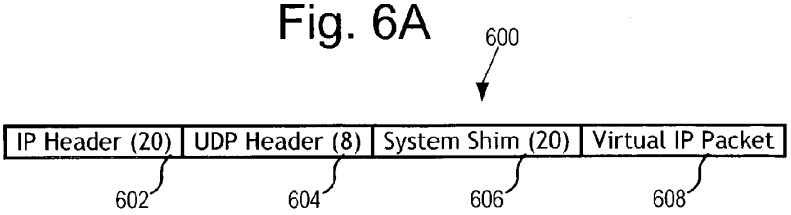


Fig. 6B

606

Field Name	Description
Protocol Version	Version information
Data Type	Type of data following Shim
Header Option Flags	Option Flag Information
Source RD Public IP	Source Route Director gIP
Dest RD Public IP	Destination Route Director gIP
Source Member pIP	Source Member Private IP
Dest Member pIP	Destination Member Private IP

Fig. 7

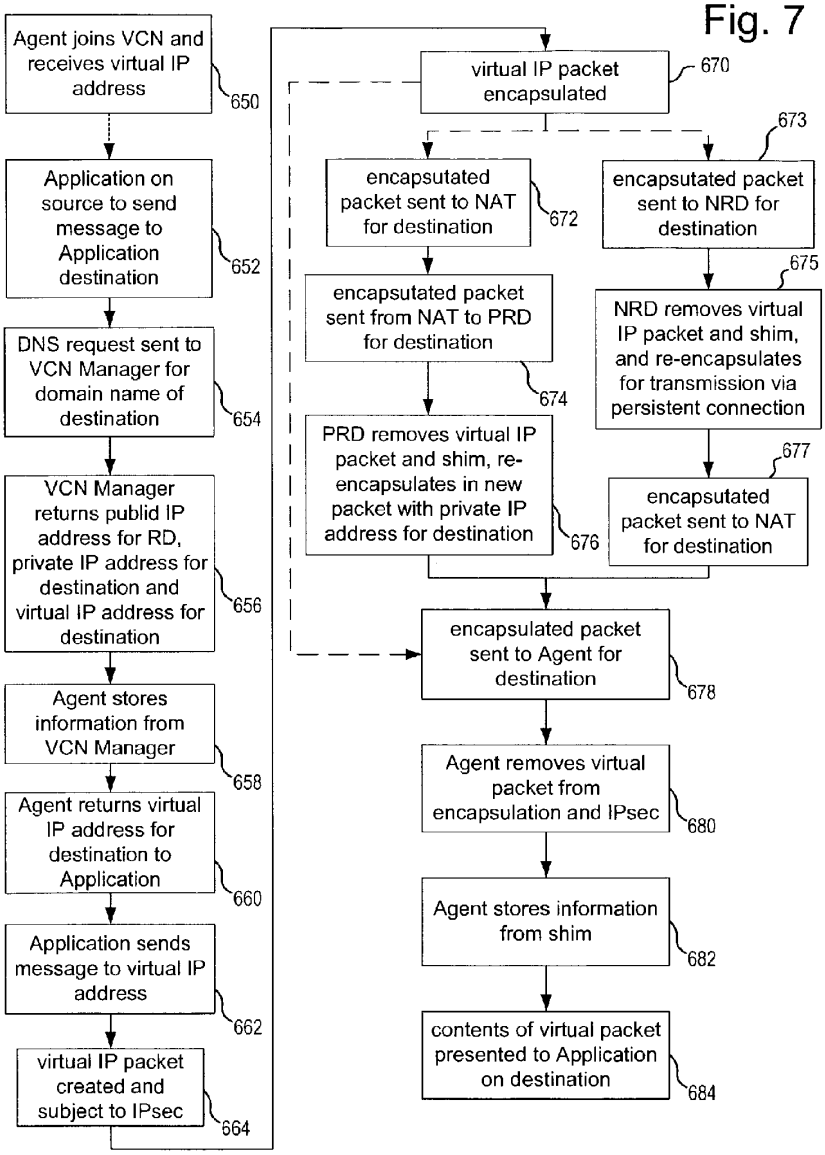

Agent joins VCN and receives virtual IP address
650
Application on source to send message to Application destination
652
DNS request sent to VCN Manager for domain name of destination
654
VCN Manager returns publid IP address for RD, private IP address for destination and virtual IP address for destination
656
Agent stores information from VCN Manager
658
Agent returns virtual IP address for destination to Application
660
Application sends message to virtual IP address
662
virtual IP packet created and subject to IPsec
664
virtual IP packet encapsulated
670
encapsutated packet sent to NAT for destination
672
673
encapsutated packet sent to NRD for destination
encapsutated packet sent from NAT to PRD for destination
674
675
NRD removes virtual IP packet and shim, and re-encapsulates for transmission via persistent connection
PRD removes virtual IP packet and shim, re-encapsulates in new packet with private IP address for destination
676
677
encapsutated packet sent to NAT for destination
encapsulated packet sent to Agent for destination
678
Agent removes virtual packet from encapsulation and IPsec
680
Agent stores information from shim
682
contents of virtual packet presented to Application on destination
684

Fig. 8

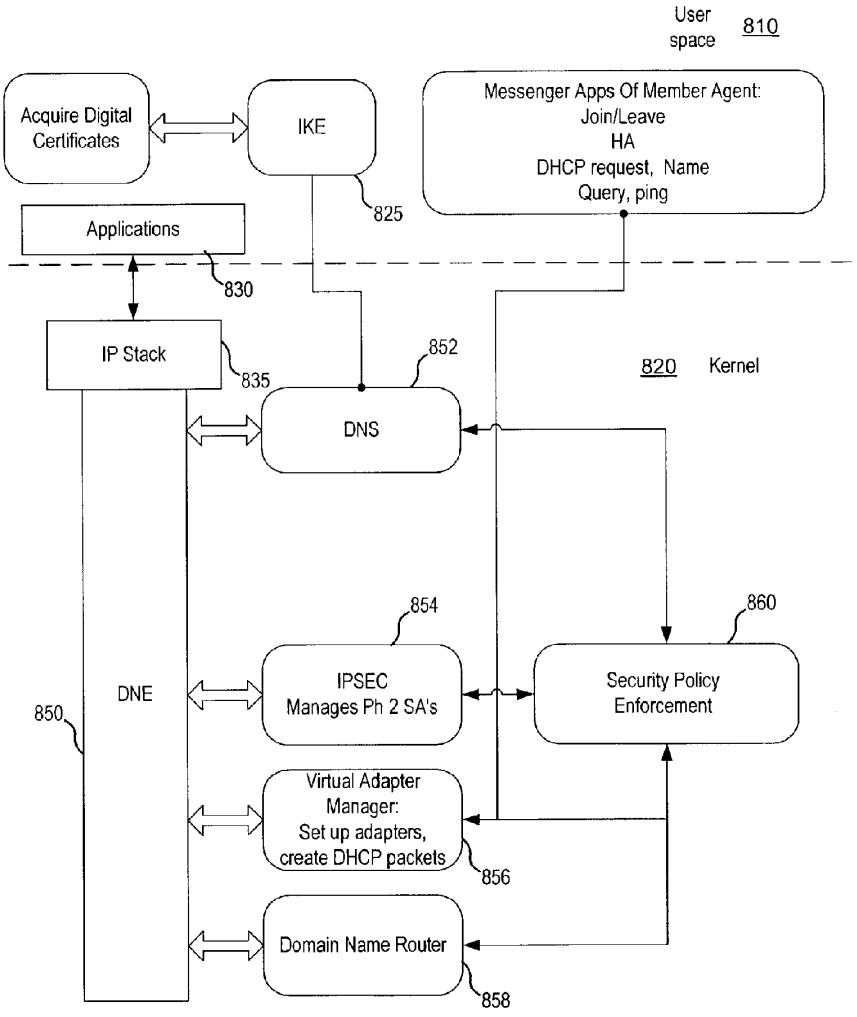

User space 810
Acquire Digital Certificates
IKE
825
Messenger Apps Of Member Agent:
Join/Leave
HA
DHCP request, Name Query, ping
Applications
830
IP Stack
835
852
820 Kernel
DNS
854
860
DNE
850
IPSEC Manages Ph 2 SA's
Security Policy Enforcement
Virtual Adapter Manager: Set up adapters, create DHCP packets
856
Domain Name Router
858

Fig. 9

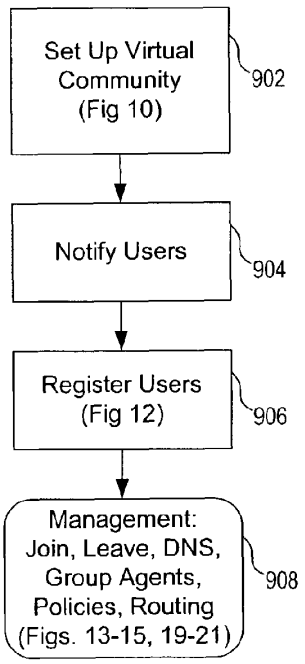

Set Up Virtual Community (Fig 10)
902
Notify Users
904
Register Users (Fig 12)
906
Management: Join, Leave, DNS, Group Agents, Policies, Routing (Figs. 13-15, 19-21)
908

Fig. 10

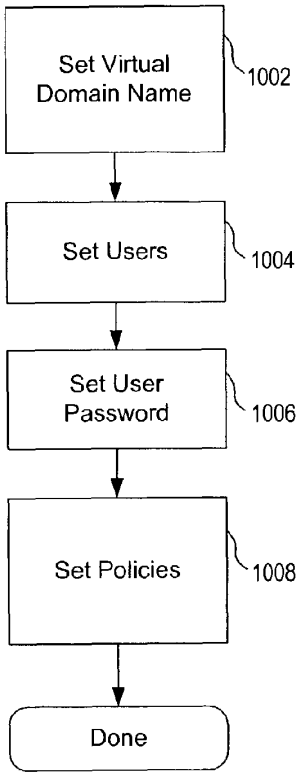

Set Virtual Domain Name
1002
Set Users
1004
Set User Password
1006
Set Policies
1008
Done

Fig. 11



Fig. 12A

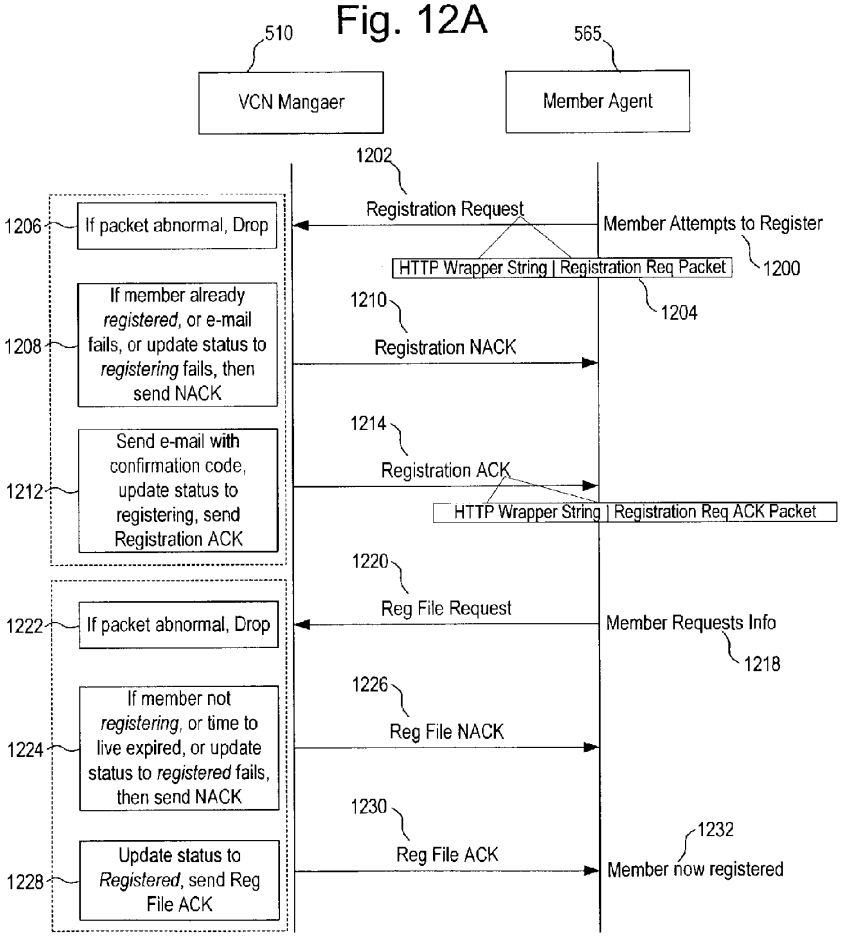


Fig. 12B

Field Name	Type	Description
Manager Seed	Array (32)	From Init Ack
Init Ack Time	Uint (8)	From Init Ack
Join Flags	Uint (2)	Indicates if rejoin and/or Group
Member Local IP	Uint (4)	The machine's local IP address
RD Local IP	Uint (4)	The Route Director local IP address
RD Global IP	Uint (4)	The Route Director Global IP
<Unused>	Uint (4)	
Member AH SPI	Uint (4)	For IPsec
Member ESP SPI	Uint (4)	For IPsec
Member Listen Port	Uint (2)	For Heartbeat Protocol
Token Timestamp	Uint (8)	The UTC time Token Key was created
Member Run ID	Array (16)	GUID Identifying current client run
Member Netbios Name	Array (16)	Microsoft NetBios support
SP Version	Uint (4)	Security Policy version
HA Version	Uint (4)	High availability version
Password Hash	Uint (20)	SHA1 of the user password string
Padding	Uint (.)	End on a multiple of 16 octets

Fig. 13

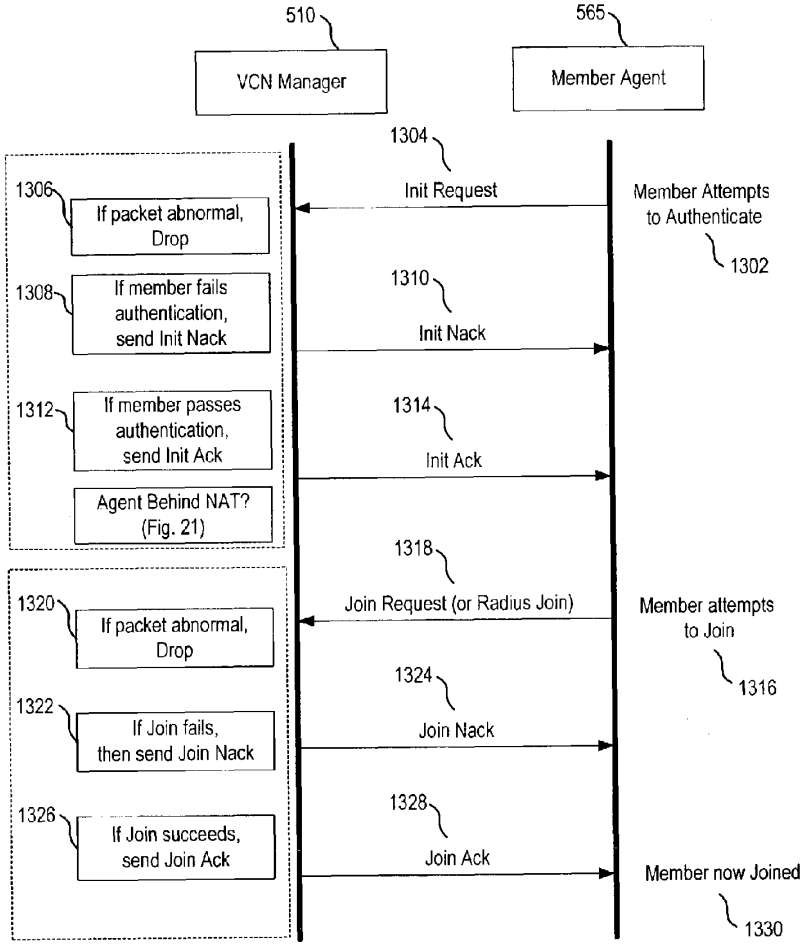

510
VCN Manager
565
Member Agent
1304
Init Request
Member Attempts to Authenticate
1302
1306
If packet abnormal, Drop
1308
If member fails authentication, send Init Nack
1310
Init Nack
1312
If member passes authentication, send Init Ack
1314
Init Ack
Agent Behind NAT? (Fig. 21)
1318
Join Request (or Radius Join)
Member attempts to Join
1316
1320
If packet abnormal, Drop
1322
If Join fails, then send Join Nack
1324
Join Nack
1326
If Join succeeds, send Join Ack
1328
Join Ack
Member now Joined
1330

Fig. 14

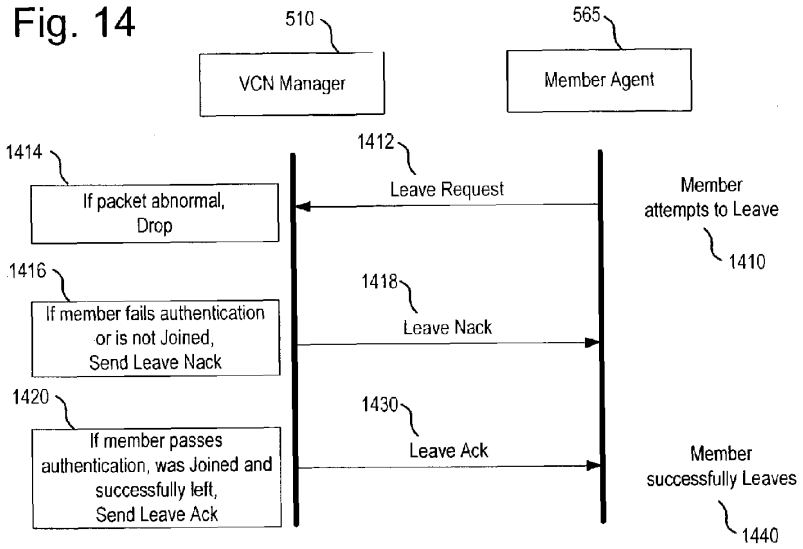

510
VCN Manager
565
Member Agent
1414
If packet abnormal, Drop
1412
Leave Request
Member attempts to Leave
1410
1416
If member fails authentication or is not Joined, Send Leave Nack
1418
Leave Nack
1420
If member passes authentication, was Joined and successfully left, Send Leave Ack
1430
Leave Ack
Member successfully Leaves
1440

Fig. 20

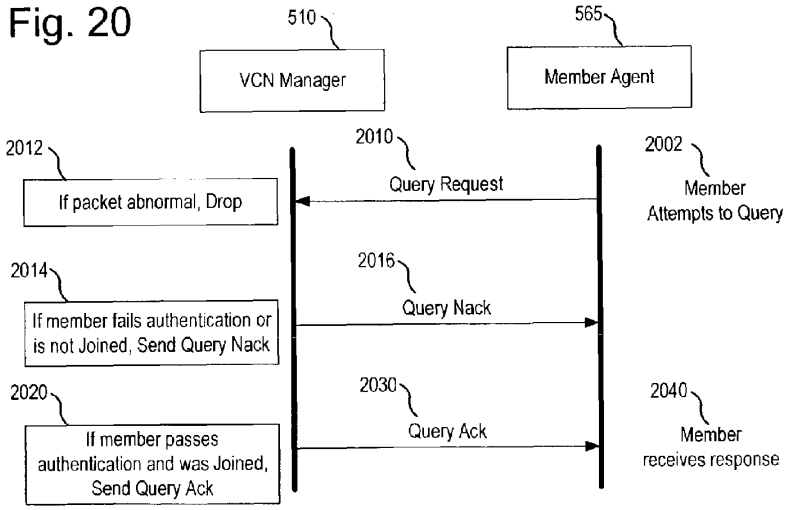

510
VCN Manager
565
Member Agent
2012
If packet abnormal, Drop
2010
Query Request
2002
Member Attempts to Query
2014
If member fails authentication or is not Joined, Send Query Nack
2016
Query Nack
2020
If member passes authentication and was Joined, Send Query Ack
2030
Query Ack
2040
Member receives response

Fig. 15

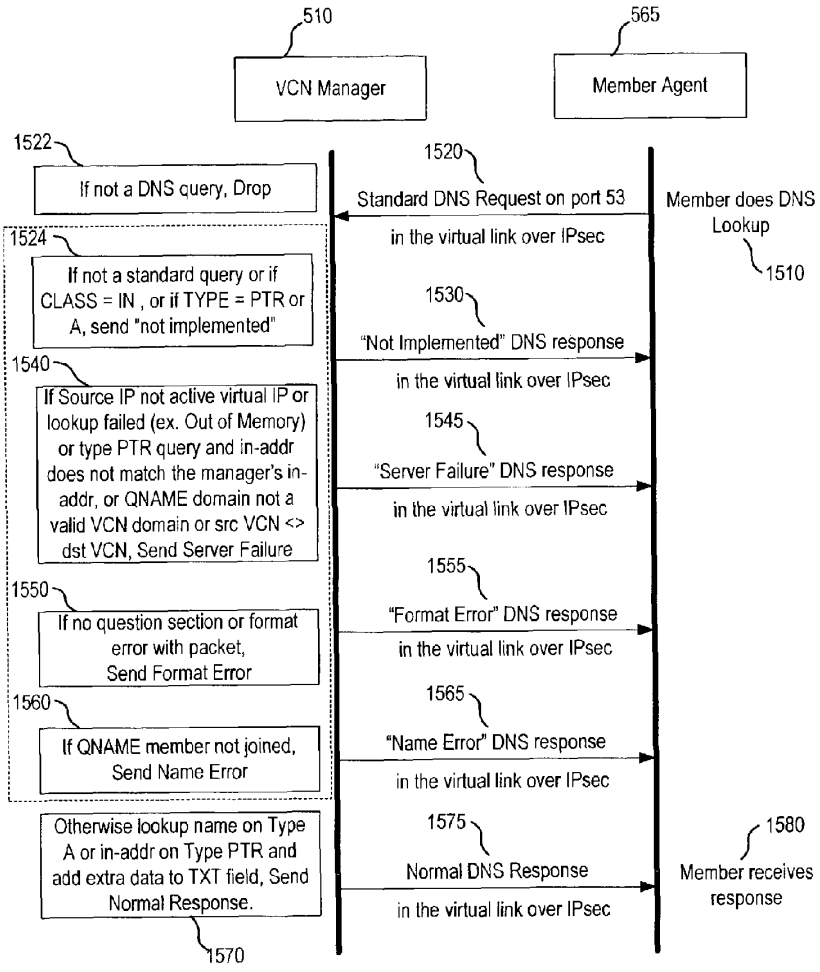

510
VCN Manager
565
Member Agent
1522
If not a DNS query, Drop
1520
Standard DNS Request on port 53
in the virtual link over IPsec
Member does DNS Lookup
1510
1524
If not a standard query or if CLASS = IN , or if TYPE = PTR or A, send "not implemented"
1530
"Not Implemented" DNS response
in the virtual link over IPsec
1540
If Source IP not active virtual IP or lookup failed (ex. Out of Memory) or type PTR query and in-addr does not match the manager's in-addr, or QNAME domain not a valid VCN domain or src VCN <> dst VCN, Send Server Failure
1545
"Server Failure" DNS response
in the virtual link over IPsec
1550
If no question section or format error with packet, Send Format Error
1555
"Format Error" DNS response
in the virtual link over IPsec
1560
If QNAME member not joined, Send Name Error
1565
"Name Error" DNS response
in the virtual link over IPsec
Otherwise lookup name on Type A or in-addr on Type PTR and add extra data to TXT field, Send Normal Response.
1570
1575
Normal DNS Response
in the virtual link over IPsec
1580
Member receives response

Fig. 16A

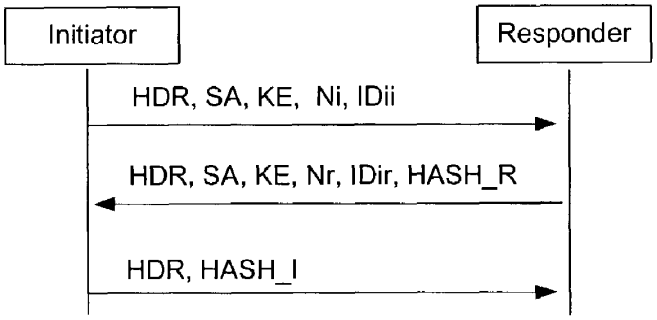


Fig. 16B

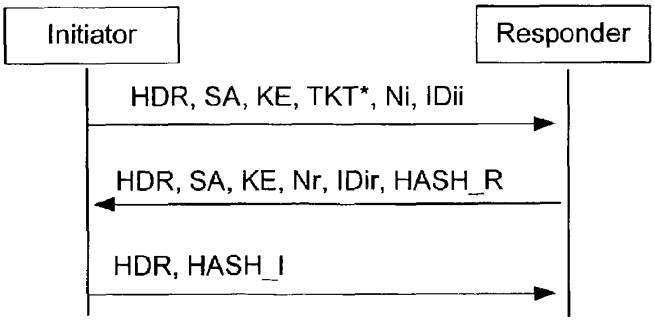


Fig. 17

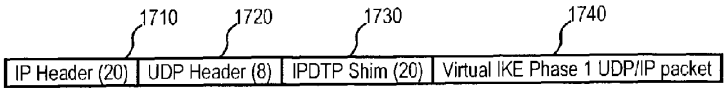


Fig. 18

IKE Ticket Payload in first IKE packet — 1740

Field Name	Field Type (Octets)	Description
Next Payload	Uint (1)	Type of payload following ours[1]
Reserved	Uint (1)	= 0, Part of ISAKMP
Payload Length (x)	Uint (2)	In octets
Payload Data	Array (x)	Payload in Network Byte Order

IKE Ticket Payload Data — 1750

Field Name	Field Type (Octets)	Description
Total Size	Uint (2)	Size of Payload
Number of Payload Items (x)	Uint (2)	Number of Items in the Item List
Item List	Array (.) * x	List of items in payload

IKE Ticket Item (one of Item List in Payload Data)

Field Name	Field Type (Octets)	Description
Item Type	Uint (2)	One of the types shown below
Item Size (x)	Uint (2)	Size of this item in octets
Item	Array (x)	Item in packed network byte order

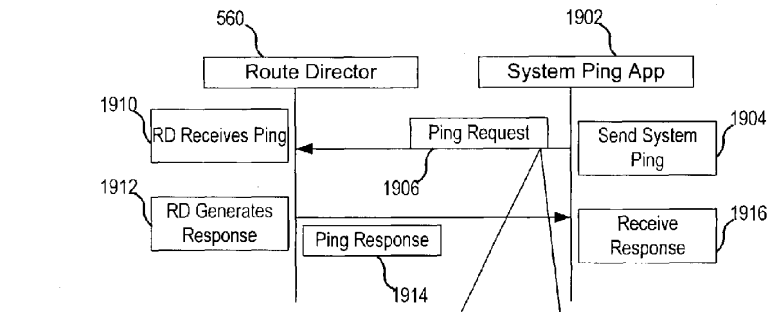
1760

IKE Ticket Payload Item Types

Item Name	Description
My FQDN	The Initiator's FQDN
My Ticket	A Ticket created by Initiator for Target
Peer FQDN	The Target's FQDN
Peer Ticket	A Ticket created by Manager for Target

1770

Fig. 19



IP Header (20)	UDP Header (8)	System Shim (20)	System Ping (4)

Field Name	Description
Protocol Version	Version
Data Type	= 1 for Information Ping to RD
Header Option Flags	None
Source RD Public IP	Source Route Director gIP = 0
Dest RD Public IP	Destination RD gIP = 0
Source member pIP	Source member private IP = 0
Dest member pIP	Destination member private IP = 0

Field Name	Description
Type	IPDTP Ping Type
Sequence	Arbitrary Sequence Number

Fig. 21

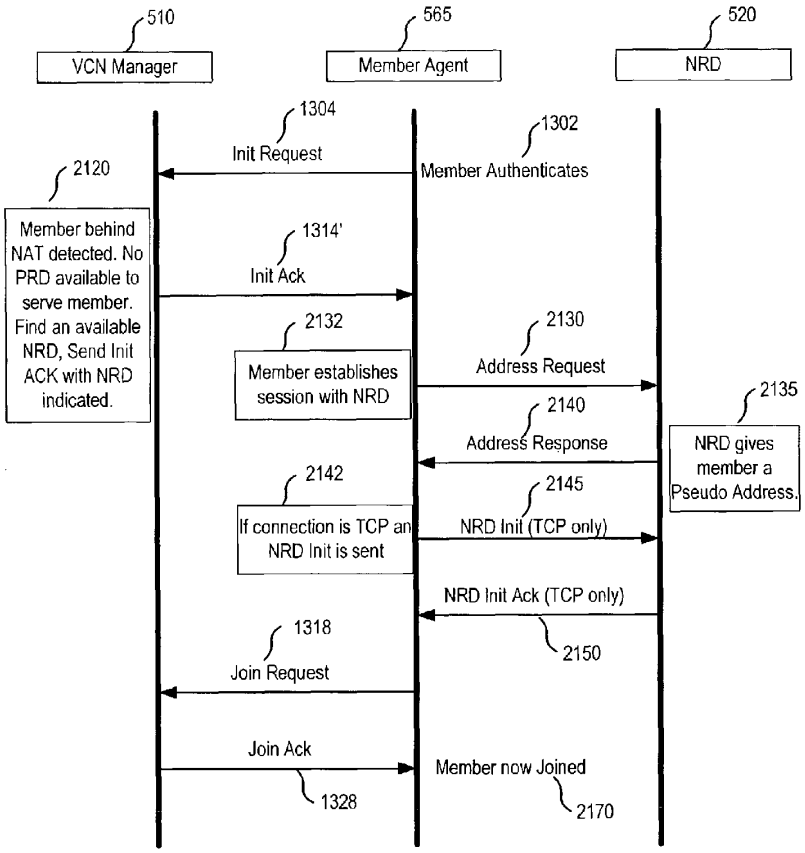

510
VCN Manager
565
Member Agent
520
NRD
1304
Init Request
1302
Member Authenticates
2120
Member behind NAT detected. No PRD available to serve member. Find an available NRD, Send Init ACK with NRD indicated.
1314'
Init Ack
2132
Member establishes session with NRD
2130
Address Request
2135
2140
Address Response
NRD gives member a Pseudo Address.
2142
If connection is TCP an NRD Init is sent
2145
NRD Init (TCP only)
NRD Init Ack (TCP only)
2150
1318
Join Request
Join Ack
1328
Member now Joined
2170

Fig. 22

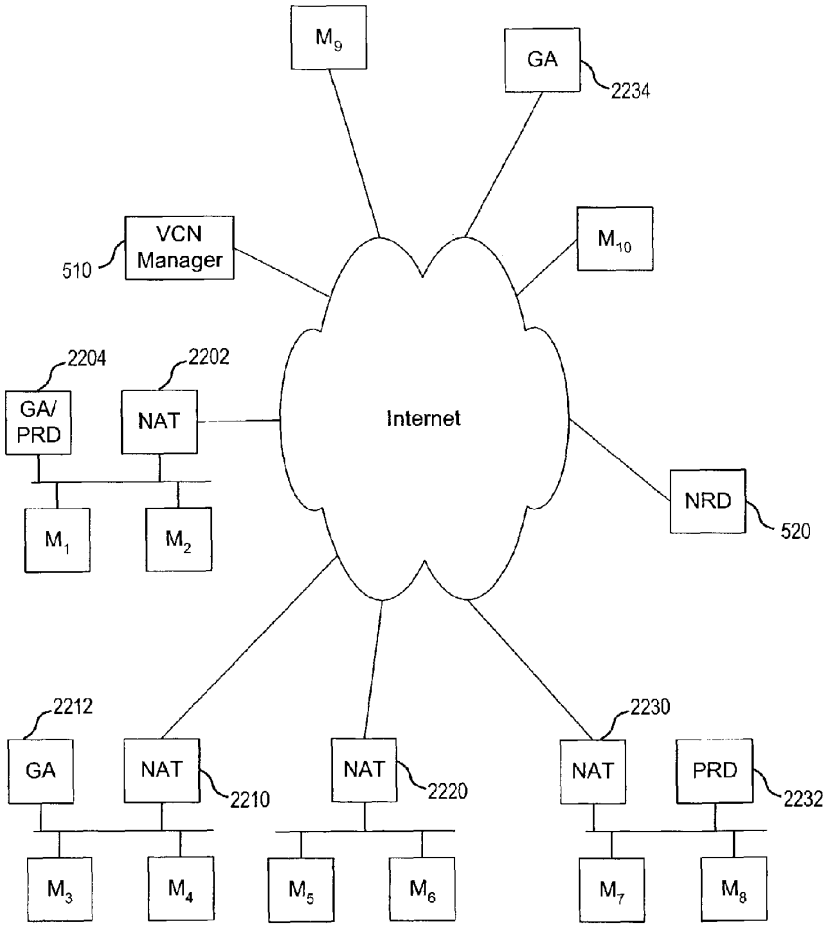

M9
GA
2234
VCN Manager
510
M10
2204
2202
GA/ PRD
NAT
Internet
NRD
520
M1
M2
2212
2230
GA
NAT
2210
NAT
2220
NAT
PRD
2232
M3
M4
M5
M6
M7
M8

Fig. 23

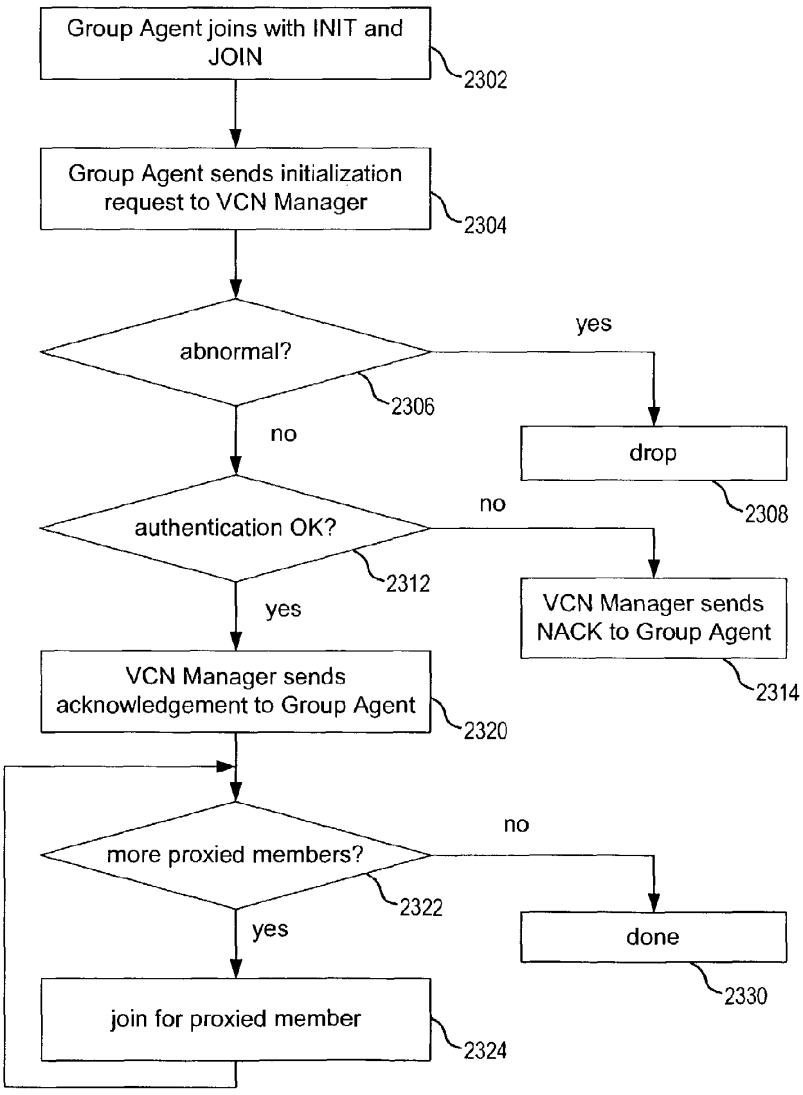

Group Agent joins with INIT and JOIN
2302
Group Agent sends initialization request to VCN Manager
2304
abnormal?
2306
yes
drop
2308
no
authentication OK?
2312
no
VCN Manager sends NACK to Group Agent
2314
yes
VCN Manager sends acknowledgement to Group Agent
2320
more proxied members?
2322
no
done
2330
yes
join for proxied member
2324

Fig. 24

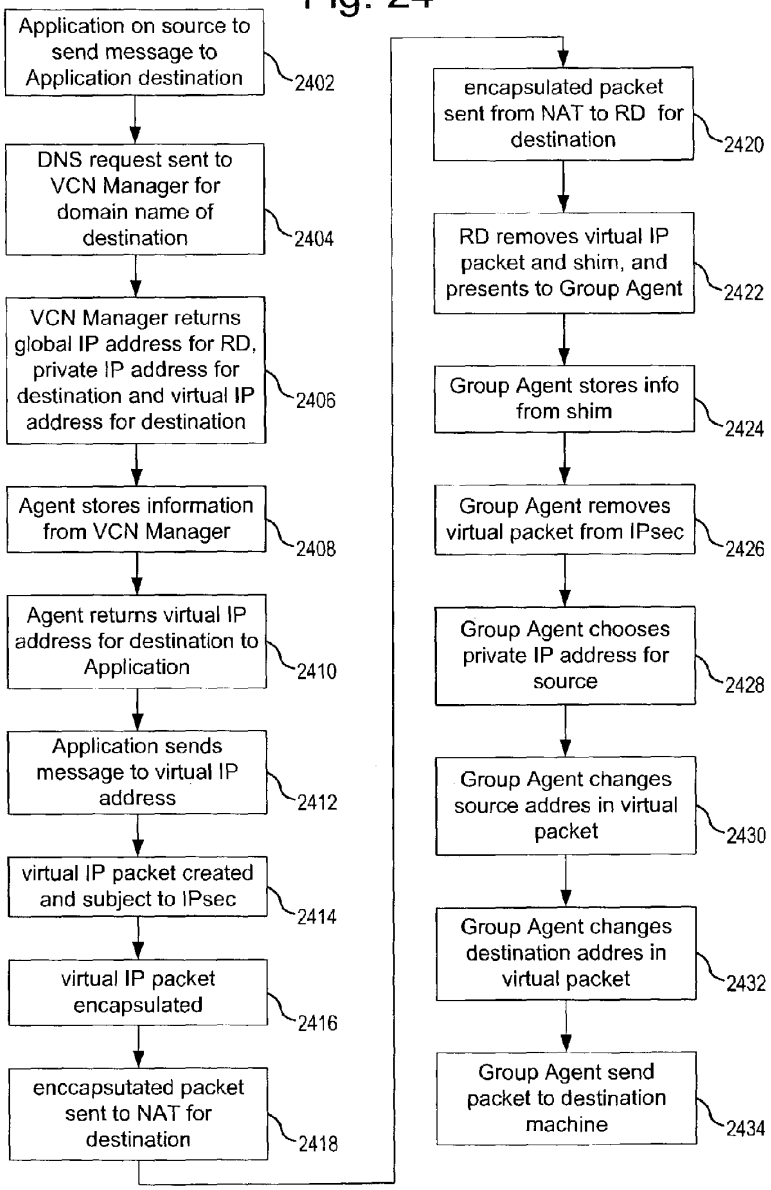

Application on source to send message to Application destination
2402
DNS request sent to VCN Manager for domain name of destination
2404
VCN Manager returns global IP address for RD, private IP address for destination and virtual IP address for destination
2406
Agent stores information from VCN Manager
2408
Agent returns virtual IP address for destination to Application
2410
Application sends message to virtual IP address
2412
virtual IP packet created and subject to IPsec
2414
virtual IP packet encapsulated
2416
enccapsutated packet sent to NAT for destination
2418
encapsulated packet sent from NAT to RD for destination
2420
RD removes virtual IP packet and shim, and presents to Group Agent
2422
Group Agent stores info from shim
2424
Group Agent removes virtual packet from IPsec
2426
Group Agent chooses private IP address for source
2428
Group Agent changes source addres in virtual packet
2430
Group Agent changes destination addres in virtual packet
2432
Group Agent send packet to destination machine
2434

Fig. 25

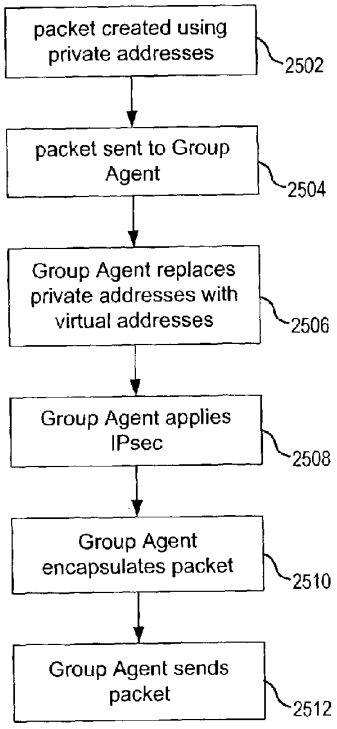
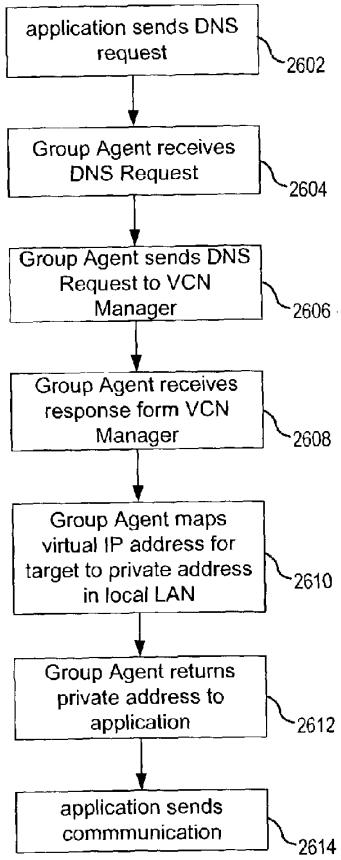

packet created using private addresses
2502
packet sent to Group Agent
2504
Group Agent replaces private addresses with virtual addresses
2506
Group Agent applies IPsec
2508
Group Agent encapsulates packet
2510
Group Agent sends packet
2512

Fig. 26


application sends DNS request
2602
Group Agent receives DNS Request
2604
Group Agent sends DNS Request to VCN Manager
2606
Group Agent receives response form VCN Manager
2608
Group Agent maps virtual IP address for target to private address in local LAN
2610
Group Agent returns private address to application
2612
application sends commmunication
2614

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This Application is related to the following Applications: U.S. Pat. No. 7,139,828 issued Nov. 21, 2006; U.S. patent application Ser. No. 10/161,573, "Creating A Public Identity For An Entity On A Network," filed on Jun. 3, 2002; U.S. patent application Ser. No. 10/233,288, "Communicating With An Entity Inside A Private Network Using An Existing Connection To Initiate Communication," filed on Aug. 30, 2002; U.S. patent application Ser. No. 10/403,829 "Secure Virtual Address Realm," filed on Mar. 31, 2003; and U.S. patent application Ser. No. 10/403,518 "Group Agent," filed on Mar. 31, 2003. All of these related applications are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention is directed to a network services system.

2. Description of the Related Art

Networked data devices provide users with efficient means for communication and collaboration. In recent years, the Internet has played a central role in allowing different types of networked devices to connect and share information across a myriad of networks. As technology advances and more organizations and people rely on the Internet, new challenges are presented for enhancing the ability to communicate. One such challenge is to enable the rapid creation of a secure means that allows local and remote specified entities to communicate and collaborate from any location via a standard Internet connection. For any solution to be widely accepted, it must take into account the realities and limitations currently existing.

For communication on the Internet, the Internet Protocol (IP) has become the default protocol used by most hosts and to which communication applications are now written. To transmit data from a source to a destination, the Internet Protocol uses an IP address. An IP address is four bytes long and consists of a network number and a host number. When written out, IP version 4 addresses are specified as four numbers separated by dots (e.g. 198.68.70.1). Users and software applications do not always refer to hosts or other resources by their numerical IP address. Instead of using numbers, they use ASCII strings called domain names. The Internet uses a Domain Name System (DNS) to convert a domain name to an IP address.

The Internet Protocol has been in use for over two decades. It has worked extremely well, as demonstrated by the exponential growth of the Internet. Unfortunately, the Internet is rapidly becoming a victim of its own popularity, it is running out of addresses.

One popular solution to the depleting address problem is Network Address Translation (NAT). This concept includes predefining a number of network addresses to be private addresses and public addresses. Public addresses are unique addresses that should only be used by one entity having access to the Internet. That is, no two entities on the Internet should have the same public address. Private addresses are not unique and are typically used for entities not having direct access to the Internet. Private addresses are used in private networks. Private addresses can be used by more than one organization or network. NAT assumes that all of the machines on a network will not need to access the Internet at all times. Therefore, there is no need for each machine to have a public address. A local network can function with a small number of one or more public addresses assigned to a NAT device. The remainder of the machines on the network will be assigned private addresses. Since entities on the network have private addresses, the network is considered to be a private network.

When a particular machine having a private address on the private network attempts to initiate a communication to a machine outside of the private network (e.g. via the Internet), the NAT device will intercept the communication, change the source machine's private address to a public address and set up a table for translation between public addresses and private addresses. The table can contain the destination address, port numbers, sequencing information, byte counts and internal flags for each connection associated with a host address. Inbound packets are compared against entries in the table and permitted through the NAT device only if an appropriate connection exists to validate their passage. One problem with a many NAT implementations is that it only works for communication initiated by a host within the private network to a host on the Internet that has a public IP address. Many NAT implementations will not work if the communication is initiated by a host outside of the private network and is directed to a host with a private address in the private network.

For most organizations, the security of devices coupled to the Internet is a concern. As a result, not all devices are directly connected to or accessible via the Internet. Rather, many devices are placed in private networks for security concerns (in addition to the address usage issue described above). Many private networks are secured by placing a firewall device between the private network and the Internet.

Another problem with many current communication schemes is that mobile computing devices can be moved to new and different networks, including private networks. These mobile computing devices may need to be reachable so that a host outside of the private network can initiate communication with the mobile computing device. However, in this case the problem is two-fold. First, there is no means for allowing the host outside of the private network to initiate communication with the mobile computing device. Second, the host outside the private network does not know the address for the mobile computing device or the network that the mobile computing device is currently connected to.

Thus, there is a need for a system that provides for local and remote entities to communicate and collaborate using the Internet, can work with existing NAT devices and firewalls, and allows for devices to move to different physical networks. To increase the ability of such a system to be accepted by the Internet community, it is desirable for such a system to not require changes to existing applications, allow peer-to-peer applications to communicate directly across the Internet and to not require changes to existing protocols. Each of these issues will be discussed below.

Large amounts of resources have been used to purchase and deploy existing applications currently running on the millions of computing devices. Organizations and individuals are not likely to want to adopt new communications solutions that require them to absorb the additional cost of replacing all of their applications.

To provide efficient and secure communication, it is desirable for devices to have the ability to allow their IP based applications to communicate directly with each other. By allowing peer-to-peer applications to communicate directly across the Internet, security is enhanced since the recipient is specifically identified and communication is passed directly between the applications on two or more respective machines.

AA/SWA Ex. 1015, p.341 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Most machines on the Internet use the TCP/IP (Transmission Control Protocol/Internet Protocol) reference model to send data to other machines on the Internet. The TCP/IP reference model includes four layers: the physical and data link layer, the network layer, the transport layer, and the application layer. The physical layer portion of the physical and data link layer is concerned with transmitting raw bits over a communication channel. The data link portion of the Physical and Data Link layer takes the raw transmission facility and transforms it into a line that appears to be relatively free of transmission errors. It accomplishes this task by having the sender break the input data up into frames, transmit the frames and process the acknowledgment frames sent back by the receiver.

The network layer permits a host to inject packets into a network and have them travel independently to the destination. On the Internet, the protocol used for the network layer is the Internet Protocol (IP).

The transport layer is designed to allow peer entities on the source and destination to carry on a "conversation." On the Internet, two protocols are used. The first one, the Transmission Control Protocol (TCP), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to he delivered without error to another machine on the Internet. It fragments the incoming byte stream into discrete segments and passes each one to the network layer. At the destination, the receiving TCP process reassembles the received segments into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more segments than it can handle. The second protocol used in the transport layer on the Internet is the User Datagram Protocol (UDP), which does not provide the TCP sequencing or flow control. UDP is typically used for one-shot, client server type requests-reply queries for applications in which prompt delivery is more important than accurate delivery.

The transport layer is typically thought of as heing ahove the network layer to indicate that the network layer provides a service to the transport layer. Similarly, the transport layer is typically thought of as being below the application layer to indicate that the transport layer provides a service to the application layer.

The application layer contains the high level protocols, for example, Telnet, File Transfer Protocol (FTP), Electronic Mail-Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP).

FIG. **1** depicts the basic structure of an IP version 4 packet **10** used at the Network Layer. IP packet **10** consists of header **12** and payload **14**. Payload **14** stores the data received from the Transport Layer in the TCP/IP model. FIG. **2**A depicts the format of a header of an IP packet. The header is depicted to include six rows. The first five rows are 32 hits wide. The first five rows of the header comprise a 20 byte fixed portion of the header. The last row of the header provides a variahle sized options field **22**. Version field **24** keeps track of which version of the protocol the packet belongs to. The current version used on the Internet is version 4. IHL field **26** describes the length of the header in 32 bit words. Type field **28** indicates the type of service requested. Various combinations of reliability and speed are possible. Length field **30** contains the size of the packet, including both the header and the data. Identification field **32** is needed to allow the destination host to determine which packet the received fragment belongs to. All fragments of a packet contain the same identification value. Next comes three flags, which inclnde an unused hit **33** and then two 1 hit fields **34** and **36**. DF field **34** stands for don=t fragment. It is an order to the routers not to fragment the packet hecause the destination is incapable of putting the pieces back together again. MF field **36** stands for more fragments. All fragments except for the last one have this bit set. Fragment offset field **38** indicates where in the current segment this fragment belongs. Time to Live field **40** is used to limit packet lifetime. It is supposed to count time in seconds, allowing a maximum life time of 255 seconds. In practice, it may count hops (or hops and seconds). The time is decremented on each hop by a router. When the time to live hits 0, the packet is discarded and a warning is sent back to the source using an Internet Control Messaging Protocol (ICMP) packet. This feature prevents packets from wandering around forever. Protocol Field **42** indicates which transport layer type is to receive the segment. TCP is one possibility, UDP is another. Checksum field **44** verifies the header. One method for implementing a checksum is to add up all 16 bit half words constituting the header and take the ones compliment of the result. Note that the checksum must be recomputed at each hop because the Time to Live field **40** changes or the content of the options field changes. Source field **46** indicates the IP address for the source of the packet and destination field **48** indicates the IP address for the destination of the packet. Options field **22** is a variable length field designed to hold other information. Currently, options used on the Internet indicate security, suggested routing path, previous routing path and time.

UDP is an alternative to TCP. FIG. **2**B depicts the structure of a packet that uses UDP. Like the TCP, UDP uses the Internet Protocol to actually send a data unit from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP does not provide sequencing of the packets that the data arrives in. Hence, application programs using UDP must ensure that the entire message has arrived and is in the right order. As shown in FIG. **2**B, the packet includes an IP header **12***a* and IP payload **14***a*. The payload **14***a* comprises the UDP header **50** and UDP data **60**. UDP header **50** consists of a 16 hit source port identifier, a 16 bit destination port identifier, a length field and checksum field. In FIG. **2**B, the Destination Port has a meaning within the context of a particular Internet destination address, and the Length field is the length in octets of this user datagram, including its header and the data. The checksum is the 16-bit one's complement of the sum of consecutive two octaves of a pseudo header of information from the IP header, the UDP header, and the data (padded with zero octets at the end, if necessary, to make a multiple of two octets).

In addition to using the existing Internet infrastructure, another issue in allowing public-to-private, or private-to-private, communications lies in the addressing of the devices. Where a system is coupled to the public Internet with an IP address, communication packets can be routed directly to the machine. However, many devices couple to the Internet via service providers which provide them with a dynamic IP address. Thus, those wishing to communicate with this type of user must know the constantly changing address of the user in order to communicate with them. Still other hosts may be coupled to networks that use technologies other than IP.

One solution currently in use that provides for local and remote specified entities to communicate and collaborate using the Internet is the Virtual Private Network ("VPN"). The VPN uses additional network software layers to increase security between users in the public realm and those in private realms. For example, some VPNs encrypt packets using IPsec (or other protocols). The encrypted packets are then encapsulated within a standard packet and transmitted across the Internet to the destination. At the destination, the encrypted packet is decrypted. While the existing VPN provides remote

users with secure access to a network, via the Internet, many existing VPNs have various shortcomings that prevent them from satisfying the needs of many users. For example, many VPNs do not provide for peer-to-peer communication with IPsec (or other security measures), do not work though NAT devices in all cases, are difficult to set up and maintain, do not provide for full mobility of entities communicating on the VPN, and do not always provide for communication with entities in the various private network configurations discussed herein.

One method of overcoming the mobility problem includes the use of Dynamic DNS. More information about Dynamic DNS can be found in RFC 2136 incorporated herein by reference.

Dynamic DNS is illustrated in FIG. **3**. FIG. **3** shows a first computer or device B having a host name of B.COb.com having a dynamic or static private IP address IPb and a second computer or device A having a host name of A.COa.com and having a dynamic or static private IP address IPa. Devices B and A are coupled to the Internet **506** via firewall devices **302**, **304** incorporating NAT. The addresses of B and A, as seen by devices on the Internet, are public IP addresses GIPb and GIPa, respectively. Also shown is device D, having a publicly address IPd and a host name of d.COd.com.

Also shown is a Dynamic DNS server, DDNS, residing on the Internet. In essence, the DDNS server is a DNS server supporting the dynamic DNS protocol of RFC 2136, and in this example is an authoritative name server containing records for B, A and D. The DDNS server will update it's records of B, A and D in real time, so that if or when D's address IPd changes, any query by other devices (B, A, for example) based on D's host name, will result in the response being the correct IP-IPd. Any DNS records for devices B and A will always reflect the public IP addresses (GIPa and GIPb) of the firewall/NAT devices.

Unfortunately, DDNS technology is complex and difficult to implement securely—two factors that have dramatically slowed the rate of deployment of Dynamic DNS. As a result, VPNs have not been able to adopt DDNS to solve all of the problems discussed herein.

Hence, a system is desired that allows local and remote entities to communicate and collaborate from any location via a standard Internet connection and which solves the problems discussed above.

SUMMARY OF THE INVENTION

A system is disclosed that allows local and remote entities to communicate and collaborate from various locations. In one embodiment, the system makes use of a virtual subnet with a virtual address realm. The virtual address realm allows two or more users to communicate securely via at least one public network, whether the users are both coupled directly to the public network, both coupled directly to separate private networks or whether one is in a public network and one is in a private network. The virtual address realm uses virtual addresses to identify the devices on the virtual subnet. Although the devices are in different physical subnets, from the point of view of the applications the devices of the virtual subnet appear to be in one local subnet.

In one embodiment, the virtual address realm comprises a virtual address realm definition including at least a set of users. Each user accessing the virtual address realm may have at least one virtual address in the virtual address realm and at least one physical address.

Another embodiment of the present invention comprises a virtual community network for transmitting communications via at least one physical network. The virtual community network comprises a virtual address realm including a logical name assignment, a set of users capable of communicating in the virtual address realm, and a secure communication channel. In a further aspect, the virtual community network logical name is a domain name, and the domain name may be a fully qualified domain name or a virtual domain name. In another aspect, the set of users includes at least a first user coupled to a first private physical network and a second user coupled to a second private physical network, and the first private physical network and the second private physical network may have at least one common private physical subnet address. The physical addresses may be dynamic or static.

Yet another embodiment of the invention is a method comprising the steps of: defining a virtual address realm overlying a public address realm, the virtual address realm including at least a user set and a logical name for said user set; and routing communications between users in the user set by means of virtual address realm addresses. In a further aspect, this method includes the step of registering users in the user set as members of the virtual address realm. Further, the method may include the step of assigning each registered user a unique virtual address in the virtual address realm. The method may further include the steps of encrypting communications between devices in the realm, and/or applying at least one address realm group policy.

A further embodiment of the invention is a method for providing secure communications between two devices. The method comprises the steps of: providing a virtual realm identifier; defining a set of users for the virtual realm; registering users in the realm; assigning virtual addresses; and routing information between users in said virtual address realm.

A still further embodiment of the invention comprises one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices. In this embodiment, said processor readable code is for programming one or more processors to perform a method comprising the steps of: providing a virtual address realm configuration including a user set and a domain name for said user set; and routing communications between users in said virtual address realm.

Another embodiment of the invention comprises a method for providing a secure virtual network. The method may include the steps of: providing a virtual network manager coupled to a public network; defining a member set of users entitled to communicate in the virtual network; registering members with the manager; assigning members a virtual address; and routing network traffic between the members in the virtual community.

An additional further embodiment of the invention may comprise one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices. The processor readable code may be for programming one or more processors to perform a method comprising the steps of: managing a virtual community network realm; defining a member set of users entitled to communicate in the virtual community; registering users with the virtual community; assigning each user a virtual address; and routing network traffic between the users in the virtual community.

Another embodiment of the invention is a virtual community network system. The system includes a virtual network manager including at least one virtual community definition comprising at least a domain name and a user set; and at least one route director capable of communicating with users in the user set.

In a further aspect, the virtual community network includes a communication agent installed on a device. The agent may comprise a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address.

For some devices, additional software or hardware cannot be installed on a member device or it is not desirable to install such additional software or hardware on the device. For such devices, a Group Agent can be used. The Group Agent acts as a proxy for one or more members of a virtual community without requiring installation of member agent software on the client devices.

One embodiment of a system that uses a Group Agent includes communicating with a first client and acting as an intermediary between the first client and members in a first virtual address realm so that the first client can communicate in the first virtual address realm. Note that in this embodiment the first client is not configured to communicate in the first virtual address realm. For example, no software is installed on the client to add drivers, layers or interfaces specific to the first virtual address realm.

Another embodiment of a system using a Group Agent includes communicating messages with a first client and communicating the messages with members in a virtual address realm on behalf of the first client. While communicating with the first client, the messages do not use virtual addresses. During the communication process, the messages are transformed so that the messages include virtual addresses when communicating with members in the virtual address realm and the messages do not include virtual addresses when communicating with the first client.

In one implementation, the first entity resides in a first physical address realm and the second entity resides in a second physical address realm, where the first physical address realm overlaps with the second physical address realm. For example, consider the situation where the first physical address realm is a first private network using a first set of private addresses and the second physical address realm is a second private network using a second set of private addresses, where there are private addresses that exist in both the first set of private addresses and the second set of private addresses.

The present invention can be accomplished using hardware, software, or a combination of both hardware and software. The software used for the present invention is stored on one or more processor readable storage media including hard disk drives, CD-ROMs, DVDs, optical disks, floppy disks, tape drives, RAM, ROM or other suitable storage devices. In alternative embodiments, some or all of the software can be replaced by dedicated hardware including custom integrated circuits, gate arrays, FPGAs, PLDs, and special purpose computers. In one embodiment, software implementing the present invention is used to program one or more processors. The processors can be in communication with one or more storage devices, peripherals and/or one or more communication interfaces.

These and other objects and advantages of the present invention will appear more clearly from the following description in which the preferred embodiment of the invention has been set forth in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described with respect to the particular embodiments thereof. Other objects, features, and advantages of the invention will become apparent with reference to the specification and drawings in which:

FIG. **1** depicts an IP packet.

FIG. **2**A depicts the format of a header of an IP packet.

FIG. 2B depicts the format of a UDP packet.

FIG. **3** depicts a print-out implementation of a dynamic routing system.

FIG. **4** depicts a block diagram of an implementation of the system of the present invention.

FIG. **5**A is a structural network block diagram illustrating elements used in the system of the present invention.

FIG. 5B is a logical block diagram depicting communication types in an implementation of the system of the present invention

FIG. **6**A depicts a packet structure for a communication packet in accordance with the present invention.

FIG. 6B is a table depicting the shim configuration of the packet in FIG. **6**A.

FIG. **7** is a flow chart describing the overall process for communicating.

FIG. **8** is a block diagram illustrating the structure of the Member Agent application in the system of the present invention.

FIG. **9** is a flowchart illustrating the steps which occur in the creation of a virtual community.

FIG. **10** is a flowchart illustrating the process of configuring a virtual community.

FIG. **11** depicts an HTTP wrapper structure.

FIG. **12**A is a flow diagram depicting a user registration process of the present invention.

FIG. 12B is a table illustrating the structure of the registration file information structure.

FIG. **13** is a flowchart depicting a member join process in accordance with the present invention.

FIG. **14** is a flowchart depicting a member leave request in accordance with the present invention.

FIG. **15** is a flow diagram depicting DNS request for a member in the virtual community in accordance with the present invention.

FIG. **16**A depicts the commonly used IKE phase one aggressive mode exchange.

FIG. 16B depicts the IKE phase one aggressive mode exchange used in accordance with the present invention.

FIG. **17** depicts a packet structure of the virtual IKE phase 1 packet.

FIG. **18** depicts the IKE ticket payload data structure.

FIG. **19** is a representation of a system ping sequence in accordance with the present invention.

FIG. **20** is a flow diagram depicting a query request in the system of the present invention.

FIG. **21** depicts a flow structure for addressing and routing conducted by a Route director.

FIG. **22** is a block diagram depicting one embodiment of various components of the present invention utilizing a Group Agent.

FIG. **23** is a flow chart describing one embodiment of the process for Group Agent initialization.

FIG. **24** is a flow chart describing one embodiment of a process for initiating communication with a member that is using a Group Agent.

FIG. **25** is a flow chart describing one embodiment of a process for communicating using a Group Agent.

FIG. **26** is a flow chart describing one embodiment of a process for initiating communication by a member that is using a Group Agent.

DETAILED DESCRIPTION

One embodiment of the present invention provides for a secure Virtual Community Network or "VCN." In essence, a

VCN is a private dynamic network which acts as a private LAN for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. Thus, the invention provides a separate private virtual address realm, seen to each user as a private network while seamlessly crossing public and private network boundaries.

A basic overview of the system is shown in FIG. **4**. FIG. **4** shows a computer or device B (host name—b.COb.com) in a first private domain and computer or device A (host name—a.COa.com) in a second private domain, both of which are coupled to the Internet by firewall devices **402**, **404**. The firewall devices are configured to implement Network Address Translation (NAT). A and B have dynamic or static private IP addresses. Computer or device X is coupled directly to the public Internet and has a public IP address.

In the present invention, a virtual community network (VCN) X.VCN is formed. Machines A, B and X can join the VCN, leave the VCN, or allow other machines in the VCN to communicate with them. More than simply a virtual private network (VPN), all members of the VCN are accessible as if they were part of a physical local network. The application running on the members of the VCN can accomplish what they would be able to accomplish if they were on the same physical routed network (e.g. all in the same private network). Membership in the VCN is controlled by an administrator via an administrative interface. In general, the administrator defines certain aspects of the VCN and then invites members into the VCN by specifying the domain name for each member. Members then register themselves with a VCN Manager, and notify the Manager via join and leave requests when they are available to participate in the community. Once registered and joined, members can communicate with other members as though connected via a local LAN.

As shown in FIG. **4**, A, B and X may all make direct connections to each other through communications within the virtual domain. In FIG. **4**, dashed lines represent direct communication paths seen to applications running on A, B and X, all "seeing" the virtual addresses of each other and communicating with each other using the application's IP interface.

A hardware architecture for the machines, server or other devices used to implement the present invention should be well understood to one of average skill in the art. Suitable hardware includes one or more processors, a memory, a mass storage device, a portable storage device, a first network interface, a second network interface and I/O devices, in communication with each other. The choice of processor is not critical as long as a suitable processor with sufficient speed is chosen. The memory can be any conventional computer memory. The mass storage device can include a hard drive, CD-ROM or any other mass storage device. The portable storage can include a floppy disk drive or other portable storage device. If the computer is acting as a router, it includes two or more network interfaces. In other embodiments, the computer may include only one network interface. The network interface can include a network card for connecting to an Ethernet or other type of LAN. In addition, one or more of the network interfaces can include or be connected to a firewall. For a gateway, one of the network interfaces will typically be connected to the Internet and the other network interface will typically be connected to a LAN. However, a gateway can exist physically inside a network. I/O devices can include one or more of the following: keyboard, mouse, monitor, display, printer etc. Software used to perform the methods of the present invention are likely to be stored in mass storage (or any form of non-volatile memory), a portable storage media (e.g. floppy disk or tape) and/or, at some point, in memory. The above described hardware architecture is just one suitable example depicted in a generalized and simplified form. The present invention could include dedicated hardware, a dedicated router with software to implement the invention or other software and/or hardware architectures that are suitable.

A more detailed overview of one embodiment of the present invention is depicted in FIGS. **5**A and **5**B. FIG. **5**A illustrates various embodiments of devices coupled to public and private networks in a manner which allows use of the present invention, and is a representation of a physical connection of such devices. FIG. **5**B illustrates a logical representation of elements used to create a VCN and of the various formats of communication traffic between those elements shown in FIG. **5**A.

Specifically, FIGS. **5**A and **5**B illustrate various user machines M_n coupled to the Internet **506**, as well as other devices, described below, which implement a virtual community in accordance with the present invention. Devices M_n can be personal computers, servers or other computing devices (mobile or non-mobile). Each machine may have different communication connectivity with the Internet.

In general, an exemplary system for implementing a VCN in accordance with the invention comprises a VCN Manager **510**, a Network Route Director **520** and/or Private Route Director **530**, and a number of Member Agents **565**. Communication between systems in various protocols is illustrated by dashed lines (UDP) and solid lines (TCP). The VCN manager and Network Route Director are shown in FIG. **5**A as being coupled directly to Internet **506**.

User devices M_A and M_E are connected to the Internet and have public IP addresses. These addresses may be dynamic or static. If static, M_A and M_E can easily communicate with each other in a manner well known in the art by simply addressing IP packets directly to each other. If the addresses are dynamic, then M_A and M_E require some means of knowing when the IP address of the other changes in order to communicate. As described below, the VCN system provides such a means.

Device M_B is in a private domain (e.g. private network)) **540** and connected to a NAT Device **515** to access the Internet **506** by a private network path **540***a*. Device M_B may use have a dynamic or static IP address specific to the private domain **540**. Generally, such addresses are part of the private received IP classes which are not routable via the Internet. For example, 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 are network addresses classified for private networks. Firewall/NATdevice **515** translates Machine M_B's private IP address to a routable public IP address. NAT device **515** may include other security functions as well. M_B communicates with other non-VCN devices on the Internet via the NAT device **515**, and with other members of the VCN via Private Route Director (PRD) **530**, which is coupled to the private network path **540***a* and is a member of the private network **540**. Device M_X is also shown as connected to and a member of the private domain **540** but has a static, routable public IP addresses. As such it may communicate with devices coupled to Internet **506** in a different manner, as illustrated in FIG. **5**B.

Devices M_C and M_D are part of a second private domain (e.g. private network) **550** coupled to a second private network path **550***a*. Again, these machines have static or dynamic private IP addresses and are coupled to the Internet via a firewall/NAT device **517**, which is itself coupled to network path **550***a*.

The VCN Manager **510** is a central server or server cluster providing management services, connection services and

security services for the VCN. Each Member Agent **565** includes client agent software (or, in some embodiments, hardware) that runs on end machines and provides virtual network services. It enables the machine to he reached from public and private networks, and implements the security aspects of the system. In FIG. **5**B, machines M_A, M_B, M_C, M_D, M_E and M_X all include Member Agents and, therefore, can he members of a particular VCN.

The Network Route Director (NRD) **520** is a stand-alone unit that runs on the public side of the Internet enabling Member Agents and Group Agents (discussed below) to be reached inside one or more private networks from the public network. Private Route Director ("PRD") **530** is an element that runs inside a private network enabling access to machines inside the private network from machines outside the private network. It can run as a service on a platform offering other services such as a Windows Server.

Generally, VCNs are defined and managed by the VCN Manager **510**. Clients utilize Member Agents or Group Agents to access other client machines (M_n), in private or public realms. The NRD or PRD routes communications to Member Agents.

As described herein, three forms of communication are used in creating and implementing the VCN. TCP is used in the registration and joining processes; encapsulated UDP packets are used between elements in establishing communication between joined devices and for management traffic, and Encrypted UDP packets are used for agent-to-agent communications.

FIG. **5**B shows exemplary traffic between elements of the VCN. A first type of traffic is TCP traffic. TCP traffic is used between member agents to establish membership in the VCN (the registration process), and make the VCN manager aware they are available to communicate with other members of the VCN (the join process). In FIG. **5**B, this is represented by solid lines **513***b*, **511***b*, **523***b* and **543***b*. TCP is also used: hy the PRD **530** to establish communications with the VCN (lines **527***b*, **527***d*); and hy the member agent of device M_B to communicate with the PRD **530** (line **533***b*). TCP may also be used by devices M_C and M_D on private network **550** to communicate with each other.

Encapsulated UDP traffic is used by elements of the VCN once membership has been established and the elements are joined in the VCN for management and administrative communications. This is represented in FIG. **5**B by lines **511***a*, **513***a*, **523***a*, **527***a*, **527***c*, **523***c*, **527***e*, **521**, **543***a*, **541**, and **519**. Encrypted UDP communications are used between devices, shown in FIG. **5**B between device M_X and M_A at **525** and device M_B and M_C at **537**.

In one embodiment, secure connections are built dynamically using IPsec tunnels based on a virtual IP space that can traverse from private networks, across the Internet and into other private networks. Strong authentication and the establishment of IPsec policies at the time members join the community offers privacy and security to the members of the virtual community. This facilitates the introduction of a variety of policy-based network services with centralized management such as Virtual Private Networks for intranets and extranets, IP-telephony domains, and IP-based PDA communities.

Communication Protocol

In the present invention, an encapsulation routing protocol allows packets to traverse addressing boundaries and identifies routing endpoints by unique DNS domain names. It employs an address virtualization scheme that accomplishes hackwards compatihility with IPv4 applications. With certain optional exceptions, UDP encapsulation is used between elements of the Virtual Community.

One example of an encapsulated packet **600** is depicted in FIG. **6**A. It includes a 20 octet IP header **602**, an 8 octet UDP header **604**, a 20 octet system shim **606**, and a variable size virtual IP packet **608**. A virtual IP packet has the same format as a standard IP packet.

Members of a VCN communicate to other members of that VCN by means of virtual IP Packets **608**. Virtual IP addressing is used to establish unique connection identities for community connected devices. IPsec can (optionally) be applied to the Virtual IP Packet for end-to-end security. Virtual IP addresses are used to identify members in the community in the virtual packet and are not directly routable. Rather, they are unique identifiers of a given connection to the upper layer application. In one embodiment, virtual IP addresses are in IPV4 format.

In general, the UDP header is set for a default port. System shim **606** carries enough addressing information to allow the Route Directors to forward the tunneled packet through the various address realms on its way to the destination. Such a routing methodology is often referred to as source routing.

In order to route packets to a peer in a different addressing realm, the protocol stack knows the address of the appropriate Route Director that serves the peer's realm. the private address of the peer or a NAT address. The Member Agent obtains the information by using the VCN Manager as a DNS authority for DNS lookup operations as described below (FIGS. **13** and **21**). The DNS response from the VCN Manager will include the above-identified information in an optional text field of the response to the Member Agent.

TCP/IP connections require IP addresses to be used as connection identifiers at the user level. If an application wishes to make a connection to "m3.abcdef.com" and another to "m4.abcdef.com", it resolves both DNS identifiers into IPv4 addresses. The system cannot assign the private IP addresses of the members to he unique connection identifiers, because two members might have the same private address in different private address realms.

Assigning a virtual address to each peer designated by a DNS string solves the problem of ambiguous endpoints. These virtual addresses may be any legal IPv4 addresses, but conflicts will occur if the same addresses are used to directly designate a peer in an IPv4 network application. For instance, if 10.0.0.10 is used as a virtual address, and is also used on a member's network as the mail server, packets that are ordinarily destined to the mail server may be redirected to a random peer. In general, when choosing virtual addresses it is best to choose addresses that will not be routable to the member. Hence, each member is assigned a virtual IP address unique in the context of the virtual community and that will not conflict with any local addresses on its LAN or any public IP addresses on the Internet.

By having each member of a VCN use a virtual address, a virtual address realm is created. The virtual address realm is the set of addresses that can be used to identify and send communications to other members of the VCN. The virtual address realm is different from a physical address realm because the physical address realm is actually used to route on a physical network. The members of a VCN will all be in the virtual address ream of that VCN, but may be in different physical address realms. For example, looking at FIGS. **5**A and **5**B, M_B and M_C are in different physical address realms (e.g. **540** and **550**); however, they are both in the virtual address realm of the VCN. Another example can he seen with FIG. **4**, where A and B are in different physical address realms (Coh.com and Coa.com); however, they are both in the same

virtual address realm. Applications on members of a VCN will see the VCN as the local subnet; therefore, the VCN can be thought of as a virtual subnet. Each member of the VCN will appear to the application as an entity connected to the local subnet.

Route Directors **530** and **520** facilitate routing UDP encapsulated traffic to private address domains **540**, **550**. In general, Route Directors either have public IP addresses or addresses that are statically remapped to a public IP address. The static translation of a Route Director's IP must leave the port in the UDP header unchanged to allow the UDP encapsulated destination port number to be directly used by public members, by other Route Directors, and by private members. Route Directors **520**, **530** and VCN Manager **510** may be configured to use a non-default UDP encapsulation port. In one embodiment, all outgoing messages are sent to this port on the next destination node and all incoming messages are read from this port. As discussed below, information in a "join" packet tells Member Agents the UDP encapsulation port to use in communications to Route Directors, network managers, and other members of the community.

System Shim **606** (see FIG. **6**A) has a format given by way of example in FIG. **6**B. Protocol Version information, data type, header option flags, and Router Information are potentially stored in the Shim. (The abbreviation "gIP" stands for "global" or public IP address, indicating an Internet routable IP address). The Data Type field indicates the meaning of the optional data that may follow the Shim. This may include a Virtual IP Packet **608**, a ping to a Route Director, a request for a Network Route Director virtual address, a Route Director response with a virtual address, a member leaving and releasing a virtual address, and a member-to-Route Director packet. The shim also includes the public IP address for the source machine's Route Director, the public IP address for the destination machine's Route Director, the private IP address for the source machine and the private IP address for the destination machine. In the case where the source or destination use a public IP address, then the shim will not need to include the private addresses of the source/destination or a route director.

The system can optionally use TCP encapsulation between a member and a Route Director. If the VCN Manager determines that a Member Agent (e.g., Agent software on a member machine) and a Route Director are both able to support a TCP connection, then it may instruct the member to initiate a TCP connection with the Route Director. TCP port **80** may be used as the destination port for all TCP encapsulated messages to the Route Director, and TCP port **20202** may be used as the source port for all TCP encapsulated messages from a private member to the Route Director.

As noted above, Network Route Directors (NRDs) **520** facilitate routing traffic into and out of private address domains without requiring reconfiguration of a firewall **517** protecting the domain **550**. As in UDP encapsulation, a special field in the system join packet (explained below) tells the Member Agent which TCP encapsulation port to use as the source port. The NRD will then re-encapsulate virtual-traffic in UDP-encapsulation before passing it on to other elements of the virtual network.

Note that more than one user can use the same device, with each such user having different virtual addresses in the same or different address realms. Additionally, regardless of the number of users, one device can be in multiple virtual address realms. In some embodiments, a user can have multiple identities, each in a different address realm.

FIG. **7** is a flow chart describing the overall process for communicating between members of a VCN. Any member of a VCN can communicate with any other member of a VCN regardless of whether either of the members are behind a firewall, behind a NAT device, directly accessible via the public Internet, in a private network, etc. From the point of view of an application on a member device, all the other members appear to be on the same LAN. Thus all applications running on a member's device will think that all other members of the VCN are on the same LAN and in the same address realm (e.g. the virtual address realm of the VCN).

In step **650** of FIG. **7**, the Agent for the potential member joins the VCN and receives a virtual IP address. In order to establish or participate in communication within the VCN, a device must register with and join the VCN, thereby becoming a member of the VCN. The Agent will send a message to VCN Manager **510** and receive a virtual IP address back. The virtual IP address received is used to identify the member in the VCN. More details of step **650** as well as other portions of FIG. **7** will be discussed below. Note that there is a dotted line between step **650** and step **652**. This dotted line signifies that a lot of time can pass between step **650** and step **652**. Additionally, after step **650** is performed, it does not need to be repeated.

In step **652** of FIG. **7**, an application on the source machine (the member initiating communication) intends to send a message to an application on the destination machine (another member of the VCN). Examples of applications that can communicate on the VCN include instant messaging, email, FTP, browsers, data transfer programs, and other applications that can communicate. Consider an example when application on device M_A intends to initiate communication with an application on device M_B. Thus, M_A is the source device and M_B is the destination device. In step **654**, the application on M_A will initiate a DNS request using the domain name for M_B. This DNS request is sent to VCN Manager **510**. In step **656**, VCN Manager **510** returns the public address of the Route Director for the destination, the private address for the destination device and a virtual IP address for the destination device. In the example described above, step **656** includes returning the public IP address for private Route Director **530**, the private address for M_B and a virtual IP address for M_B. If the destination machine has a public IP address (and, thus, does not use a routing director) then step **656** will only include returning the public IP address for the destination. If the destination machine is in a private network that uses a Network Route Director (e.g., NRD **520**), then step **656** will return the public IP address for the Network Route Director.

In step **658**, the Agent for the source device, which received the information in step **656**, will store that received information. This information can be stored in a table, or any other data structure. In step **660**, the Agent for the source device will return the virtual IP address of the destination device to the application on the source device. In step **662**, the application on the source device will initiate the sending of a message/data using the virtual IP address for the destination device. In step **664**, a virtual IP packet will be created. The source IP address for the virtual IP packet will be the virtual IP address for the source device. The destination IP address for the virtual packet will be the virtual IP address for the destination device. The virtual IP packet will be in the same format as a standard IP packet. In step **664**, the newly created virtual IP packet will be subjected to IPsec (or another security means). In some embodiments, IPsec is not used. In step **670**, the virtual IP packet is encapsulated. For example, in one embodiment, the virtual IP packet is encapsulated as described above with respect to FIGS. **6**A and **6**B. This encapsulation will include shim **630**. As described above, shim **630** will include the public IP addresses for the Route Directors

for the source and destination, and the private IP addresses for the source and destination devices. If either the source or destination do not have a Route Director, the shim will not need to include that information. For example, when the source machine is M_A, there is no Route Director for the source. If the source machine was M_C, then the shim, would include the public IP address for Network Route Director **520**. If the source is M_B, the shim would include the public IP address for Private Route Director **530**.

At this point, the path of the packet will depend on whether the destination is using a Private Route Director **530**, Network Route Director **520** or has a public IP address. If the destination has a public IP address, the process moves to step **678** where the encapsulated packet is forwarded to the destination agent.

If the destination is in a private network that has a PRD, then in step **672** the encapsulated packet is sent to the NAT device for the destination. For example, the encapsulated packet is sent from M_A to NAT **515**. In step **674**, the encapsulated packet is sent from the NAT device for the LAN that includes the destination to the Route Director for the destination. For example, the encapsulated packet is sent from NAT **515** to private Route Director **530**. In step **676**, the Route Director which received the encapsulated packet will remove the virtual IP packet and the shim from the encapsulation. The Route Director will read the shim to learn the local IP address to send the packet to. The shim and virtual IP address will then be re-encapsulated into a new packet with the original virtual packet. The new outer packet includes a destination IP address equal to the private IP address of the destination device. The encapsulated packet received in step **674** will include a source IP address equal to the public IP address for M_A (or the source's Route Director) and a destination IP address equal to the public IP address for the Route Director of the destination (e.g., PRD **530**). In step **678**, the new encapsulated packet will he sent from the Route Director to the Agent for the destination device.

If the destination agent is in a private network and is using a Network Route Director, then following encapsulation the encapsulated packet is sent to the Network Route Director for the destination agent in step **673**. At step **675**, the NRD will remove the virtual IP Packet and shim and re-encapsulate them in a UDP packet for transmission through a NAT device to the destination via a persistent UDP connection between the NRD and the destination. At step **677**, the encapsulated packet is forwarded to the NAT device (via the persistent UDP connection) behind which the destination Agent resides, which will perform its own routing of the encapsulated packet to the destination Agent in step **678**.

In step **680**, the Agent will remove the shim and the virtual IP packet from the encapsulation. The virtual IP packet will be removed from IPsec (e.g. decrypted). In step **682**, the information from the shim will be stored by the Agent. In step **684**, the contents of the virtual packet will be presented to the application on the destination device. That is, the application on the destination device will receive the contents of the data payload, or at least a portion of the data payload

When the destination wishes to respond to the source or the source wishes to send additional information, the process of FIG. **7** can be repeated. However, when repeating the process of FIG. **7** between two machines where communication is already established, the steps of performing the DNS request do not need to be performed again. That is, when the destination wishes to respond, the destination will perform the steps in FIG. **7** starting at step **662**. The Agent for the destination device will already know all the information to put in the shim. Additionally, when the source device wishes to send additional information to the destination device, the source device can start FIG. **7** at step **662**. In some embodiments, however, the steps of performing the DNS request will be performed again.

Member Agent

As noted above, devices in the VCN utilize a member agent installed on the device to communicate. One unique aspect of the system of the present invention is the integration of the agent software in a typical device.

FIG. **8** illustrates the functional flow diagram of an installed agent on a device such as a computer, server or other device. Region **810** illustrates the "user space," and region **820** represents the kernel area of the components interacting with the host device.

Applications **830** interact directly with an IP stack **835** which is built on a deterministic network extender or DNE **850**. The deterministic network extender is provided by Deterministic Networks, Inc. The network extender allows one to implement any driver level functions such as IPsec, browsers, traffic redirectors, and the like, through a series of plug-ins. As shown in FIG. **8**, a number of plug-ins, including a DNS plug-in **852**, an IPsec plug-in **854**, a virtual adapter manager **856** and a domain name router **858** (see U.S. Pat. No. 6,119,171, incorporated herein hy reference) interact with the deterministic network extender **850**. The DNS plug-in processes DNS queries by applications via the stack. The virtual adapter manager allows for additional adapters to co-exist in the same device.

The DNE is an NDIS compliant module (in Windows environments) which appears as a network device spire to the protocol stack **835**. The DNE supports the TCP/IP and UDP protocols and various adaptor types. In essence, this forms a virtual network adaptor in device installations. This means that various configurations for each virtual community can be provided for each DNE. This provides the advantage that a numher of memhers or users can utilize the same device, with the device installing a different virtnal adaptor using plug-ins for the deterministic network enhancer and each user does not need to reconfigure the network settings of the machine to join each community. Each plug-in is constructed in accordance with standards promulgated by the DNE provider.

As shown in FIG. **8**, user applications interact directly with the IP stack of the virtual adapter. Each adapter provides its own stack to the device's applications. To the applications, each stack appears separate, and no separate routing of the application is required. For example, the IKE user application **825** can interact with the domain name plug-in, the IPsec plug-in, the virtual area management communicator **856**, and the security policy manager **860**. The Adapter Manager **856** allows parallel stacks for each VCN to be implemented and used on each machine. This means a user and device can helong to several VCNs without needing to re-configure IP settings to access each VCN.

VCN Definition

FIG. **9** shows the steps which occur at the VCN Manager to define and establish a virtual community. At step **902**, an administrator sets up a virtual community by providing information to the VCN Manager via a user interface (not shown). It will be understood that the user interface and the method of providing information to the VCN Manager is not critical to the system of the present invention. One particularly advantageous interface is implemented in a World Wide Web browser. The interface may be implemented using HTML, XML, Java Applets, Java Server, Active Server Pager or any of a number of well-known Web technologies. The particular information required to set up the community network is illustrated in FIG. **10**. Next, at step **904**, users who are desig-

nated by the administrator as being allowed access to the virtual community defined in step **902** are notified by any number of appropriate means. In one implementation, the users are notified by e-mail, although other forms of notification, such as verbal or personal notification, may be used. The e-mail may contain an invitation to join the community, community authentication information, a link to a location to download the Member Agent, and/or a link to the Group Agent. Next, at step **906**, using information contained in the e-mail, users register with the VCN Manager. Registration in this context means registering a machine using a Member Agent or a Group Agent with the VCN Manager. Users may be required to install the Member Agent software. The link in the notification e-mail may provide the user with a location for downloading the Member Agent software as well as instructions for installing the software. Other information, such as system password information, is provided in the e-mail. Finally, at step **908**, management of the community is handled by the VCN Manager. This includes monitoring which registered users have joined and left the system, answering DNS requests, and applying security policies, as described herein. This may include notifying new users and registering those users as the definition of the VCN changes.

FIG. **10** is a flowchart illustrating the process of setting up a virtual community which is performed by an Administrator. Initially, the Administrator sets up a virtual domain name and address domain at step **1002**. This information is used by the VCN Manager and Route Directors to allow members to communicate. Next, users are defined at step **1004**. In one embodiment, the users are defined by providing the domain names of each of the users who will be invited to participate in the VCN. At step **1006**, default passwords are set. This is the password a user first uses to access the system. The user may be forced to change the password for security reasons at a later date. Finally, at step **1008**, polices may be defined at the domain level, the user level, or for individual machines in the domain. Policies are used to allow or deny access to individual machines, services, or other users.

Member Registration

The registration process is the first step that a user and machine go through with the VCN Manager before becoming a member of a virtual community. There are two phases to member registration: a registration request and a registration file request. Registration happens outside of the IPsec tunnels because at registration time no IPsec tunnel exists for the user registering.

In one implementation, all traffic between Member Agents and the VCN Manager (with the exception of Registration and Join function traffic is encapsulated using UDP encapsulation, represented by lines **511***a*, **513***a*, **523***a*, **519**, **521**, **527***a*, **527***c*, **537**, **523***c*, **527***e*, **541**, **543***a*, **533***a* of FIG. **5**B). This encapsulated traffic will carry management traffic between the members and the VCN Manager. A service port is reserved at the VCN Manager in the virtual network for the establishment of a TCP connection between a member and the VCN Manager. A member that joins a VCN is informed of the service port as part of the join protocol. A DNS port is also open on the virtual side of the VCN Manager. In one embodiment, the VCN Manager virtual ports are TCP Port **9001** and DNS UDP Port **53**. The packets used for the initial Registration and the subsequent Join operations use TCP port **80** outside the virtual network. This is represented in FIG. **5** by the solid lines **513***b*, **511***b*, **523***b* and **543***b*.

VCN system protocol packets that are sent outside the system tunneling are HTTP wrapped and sent to the VCN Manager on TCP port **80** to facilitate NAT traversal. More information about NAT traversal will be provided below. Each packet includes a header and payload. For compatibility with firewalls, the HTTP wrapper makes the packet a SOAP-compatible XML document. Including a binary data portion after XML is consistent with Direct Internet Message Encapsulation (DIME), a proposed lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct.

The format of the HTTP wrapper from the Member Agent to the VCN Manager is shown in FIG. **11**. The wrapper includes an HTTP HEADER, XML HEADER and P-LENGTH fields. The HTTP header includes a POST HTTP field, an Identity field, a Content Type field, and a Content Length field. The XML header includes version information and packet type information. The Header includes error codes and explanations, as well as the content type and length.

The Registration exchange between the member agent and the VCN Manager is shown in FIG. **12**A. When a Member Agent **565** attempts to register at step **1200**, Member Agent **565** will send a registration request packet **1202** to the VCN Manager **510** to start registration. The packet is included in an HTTP wrapper as illustrated at **1204**. The registration packet will carry the client Fully Qualified Domain Name (FQDN) and a Diffe-Hellman Key Exchange request to the VCN Manager. The packet further includes packet version information, type and length information, a user authenticator, the length of FQDN in octets, a VCN name offset, the member's FQDN in DNS format, the length of Diffe-Hellman value in octets, and the member's initial Diffe-Hellman value.

An Initial Password is passed to the user through an outside channel, such as e-mail (or other channel). In a setting where security is a concern, an alternative method such as personal communication or encrypted e-mail may be used.

The registration authenticator is computed using the first sixteen bytes of the HMAC-SHA-1 applied to the packet data with the password hash as the key. (Normally, the HMAC-SHA-1 algorithm generates a 20-byte result; in one embodiment of the system only the first (leftmost) 16 octets are used in the MAC.) The formulas are as follows:

$$\text{HMAC-Key-Field}=\text{SHA-1}(\text{Initial Password})$$

$$\text{Authenticator}=\text{HMAC-SHA-1}_{16}(\text{HMAC-Key-Field}, \text{Data})$$

The VCN Manager will respond in one of three ways **1206**, **1208**, **1212**, to the registration packet **1202**. VCN Manager **510** will acknowledge (ACK) the packet at step **1212** with the Registration Acknowledge (ACK) packet **1214** if the member belongs to a community but its status is "not registered." The VCN Manager also sends a phase-2 confirmation code to the member's e-mail address and changes the member status to "registering." The packet will transfer a "Time To Live" value to the member which is a timeout period in seconds for hearing back from the member with the confirmation code. Phase two of registration must be completed in this time period.

If the packet is abnormal (in size, FQDN length, bad type, etc.), the authenticator check fails, the member does not exist in the database, or the VCN server is not running, the VCN Manager drops the packet in step **1206**. The packet will be not-acknowledged (NACK) **1210** if the member is already in the "registered" state, the send e-mail operation fails, the process of updating the member to the "registering" state fails, or the random generator fails in attempting to generate a confirmation code in step **208**.

Upon receiving the Registration ACK **1214**, the user will send Registration File Request Packet **1220** to the VCN Man-

ager **510** to start registration. This packet will transfer the following information to the VCN Manager: a registration file User Authenticator, the length of FQDN in octets, a VCN name Offset, and the member's FQDN in DNS format.

The registration file user Authenticator contained in the File Request packet **1220** is slightly different from the Registration Request Authenticator in packet **1202**, in that the Initial Password, passed to the user through an outside channel (e-mail for example), and the Confirmation Code, a temporary code sent in the second e-mail with a timeout to the user, are used:

HMAC-Key-Field=SHA-1(Initial Password)

User Authenticator–HMAC-SHA-116(HMAC-Key-Field,SHA-1(Confirmation Code)+Data)

The VCN Manager will send a Registration File acknowledge Packet **1230** to the member **565** in response to the Registration File Request packet **1220** in step **1228** if it is determined that the member belongs to a community. The Acknowledge Packet **1230** will transfer the following information to the member:

Crypto Type—a code indicating how the rest of the packet is encrypted. This is provided in a crypto type field preceding the registration file.

Registration File—a structure with a number of fields containing the information required by the member to successfully perform a join. It is sent encrypted using the key generated via the Diffie-Hellman key exchange.

A table representing the Registration File structure is shown in FIG. **12**B. As shown therein, the Registration File contains an Authentication Type, a File Type, a File Length definition, a Token Key, a Key Timestamp, a Key Type, a Key Length, a High Availability (HA) Version, a HA Number, Server Information and Padding. The Token key is the shared secret with the server. The Token Key is identified by the Key Type, which is normally a Diffie-Hellman type in one embodiment. The VCN Manager also changes the member status to "registered."

If at step **1224**, the member agent status is not set at "registering," or the timeout for phase 2 has expired, a NACK packet **1226** is sent. If the packet is abnormal (in size, FQDN length, bad type, etc.), the authenticator check fails, or the user does not exist in the database, or the VCN server is not running, the packet is dropped in step **1222**. While current encrypting method for the file is to generate a key/IV pair from the combined Diffie-Hellman value using a Key Derivation Function, any number of suitable substitutes may be used.

In addition to the registration authentication described above, the system uses a packet authenticator to verify communications between the VCN Manager and Agents. The Authenticator is a cryptographically strong hash of the packet keyed by a shared secret between the source and destination. The authenticator is calculated over the entire packet using the HMAC-SHA-1 algorithm. The inputs to this Authenticator are not available until after Registration. As illustrated above, during registration an Authenticator based on the user password is used. The fields used in the calculation are a Diffie-Hellman Key comprising a multi-octet random string that is the result of the Dillie-Hellman key exchange protocol, and the entire packet data, with the Authentication field zeroed out.

The Authorization Key, AuthKey, described above, is derived from Diffie-Hellman using the KDF2 function, and used for general packet Authentication. AuthKey=KDF2 (Diffie-Hellman Key)MAC−HMAC-SHA-116(AuthKey, Data). The AuthKey need be calculated only once per registration from the KDF2 of the DH key and then stored for later use. It is known as the Authentication key and is 20 octets long.

Member Join/Leave

Once a user is registered, the user can join the VCN. Once joined, the user is a member of the VCN. Joining allows the user to let the VCN Manager and other members know that the user/member is on-line and available to communicate. The Join protocol runs between a Member Agent and the VCN Manager to establish a session key with the Manager, authenticate to the Manager, and make use of connections via the Route Directors in the community.

The Member Join process is illustrated in FIG. **13**. There are two phases to the Join operation: phase one is an Initialize Request and phase two is the actual Join. At join time, the IPSec tunnel for secure communication is not established, so the first few join packets are sent outside the IPSec tunnel.

Initially, at **1302**, the Member Agent **565** will send an Init Request Packet **1304** to the VCN Manager **510** to start authentication. The packet will carry the following information to the VCN Manager:

Version Variant Mask—used to indicate optional variations of the protocol from the member to the VCN;

Token Timestamp—identifying when a Token Key was created (in seconds);

Member seed—a random number to thwart so called "man-in-the-middle" attacks;

Member Local IP—the member's Local LAN IP address; and

Client FQDN—the client's fully qualified domain name.

Again, three responses **1306**, **1308**, **1312** are possible. At step **1306**, if the packet is abnormal, it will be dropped. Similarly, if the member fails authentication, at step **1308** a NACK packet **1310** will be sent.

If the member passes authentication at **1312**, the Manager will send an acknowledgement packet **1314** to Member **565**. An AuthKey is also transmitted as part of the INIT Request Packet, and the Manager authenticates the packet by checking this against a secure key digest. The acknowledgement packet **1314** packet will transfer the following information to the member:

Version Variant Mask—version information;

Member Seed—from the Init Request to protect against playback attacks;

Manager Seed—a unique seed used to thwart man in the middle attacks;

Session AH Key used in IPsec;

Session ESP Key—used in IPsec;

Ink ACK Time a time stamp used to tie this packet to the following Join Request. There is a timeout if the Join is delayed too long;

Authentication Method—the method used for authentication;

Route Director Private IP—if member is in a private network, this is the private IP address of the Private Route Director. The value is zero if no Route Director is used;

Route Public Public IP—if member is in a private network, this is the public IP address of the Private Route Director. The value is zero if no Route Director is used;

Tunneling Port—used for UDP encapsulation Route Director Flags. Only Bits **0** and **1** currently used to direct the agent to a Private Route Director, Network Route Director with UDP, or a Network Route Director with TCP.

At step **1312** of the join process, the VCN Manager will also determine whether the Member Agent attempting to join

is behind a NAT device. The method by which this occurs is discussed below with respect to FIG. **21** and the results of this determination may force the Agent to negotiate a session with a Network Route Director which will provide a pseudo address value used as the Agent's local IP value in the Join request, discussed below. This process is discussed in depth with respect to FIG. **21**.

Following receipt of the acknowledgement packet, at step **1316**, the member will send Join Request Packet **1318**. The packet's payload includes a manager seed, the initial ACK time, join flags, the member machine's local IP address (or pseudo address), the Route Director's private IP address, the Route Director's public IP, the member AH SPI and ESP SPI, the member listen port, a token timestamp, a GUID identifying the current client run, NetBIOS name support, a password hash, version information for high availability and security policy information.

In step **1320**, the VCN Manager will drop this packet if it is abnormal. In step **1322**, the VCN Manager will send a NACK packet **1324** if the member is not in the registered state, the timeout for Join from INIT ACK has expired, or updating the member to the Joined state fails.

If the join action succeeds, then in step **1326** the VCN Manager will send an acknowledge packet **1328**. The acknowledge packet payload includes the RMI Port at the VCN Manager, the Tunneling Port, VCN Manager Authentication Header (AH), Security Parameters Index (SPI) for IPsec, VCN Manager Encapsulating Security Payload (ESP) SPI for IPsec, the UTC Time (in seconds) when the member joined, VCN Manager Heartbeat interval (in seconds), the Member Heartbeat interval (in seconds), the VCN Manager's Virtual IP address, the Manager Subnet Prefix Length, the VCN Member Subnet Prefix Length, the Route Director's private IP address, the Route Director's public IP address, an indication of the updates that follow, an update of the Token Key, an update of the Security Policies, an update of High Availability indication, and padding. The member has now joined the community at **1330**. Once the member has joined, all communications can be encrypted using IPsec.

The system of the present invention also includes RADIUS authentication support. Generally, if a member attempts to authenticate using a RADIUS server, the VCN Manager will perform the same steps as when it receives the Join Request packet except for having a RADIUS server authenticate the member. The payload for this packet is similar to the Join Request packet except that it has an additional field for RADIUS password that is used by the RADIUS server to authenticate the member.

FIG. **14** shows the sequence for leaving a VCN. Initially, at step **1410** when a Member Agent is prepared to leave the community, a Leave Request Packet **1412** will be sent to the VCN Manager **510** to start the leave process. The Leave Request Packet will carry a Leave Flag, the FQDN Length, FQDN VCN Offset and Member FQDN. Unless dropped at step **1414** or a problem exists at **1416** which would generate a NACK packet **1418**, the VCN Manager will send the Leave ACK Packet **1430** to the member in step **1420**. This packet has no payload. At step **1440**, the member has successfully left the community.

DNS/Lookups

For one member to communicate with another member, the initiating member's agent will perform a query or DNS lookup (step **654** in FIG. **7**) to determine the address of the other member, and then establish a secure communication channel between them.

The Member Agent utilizes the VCN Manager to perform lookups of other virtual members in the virtual community using DNS. The DNS operation is conducted using the DNS protocol with the VCN Manager. The member software sends a DNS query to the VCN Manager, and the manager returns information about the target member. Besides the target member's virtual IP address, the DNS response also contains additional information about the target member. While the VCN Manager accepts all DNS requests, it will only acknowledge the DNS requests of type A, which are targeted to virtual domain names in the secure virtual communities of the VCN Manager. The VCN Manager is the authoritative name server for those virtual domain names; other requests will simply be responded to with a "Server Failure."

The DNS query and response sequence is illustrated in FIG. **15**. At step **1510**, a member will request a DNS lookup by sending a DNS request **1520** to port **53** of the VCN Manager. The DNS request **1520** will result in a normal DNS response **1575** unless any of a number of failure conditions are met, shown at steps **1522**, **1540**, **1550**, and **1560**.

If the Manager receives a query on port **53** that is not a DNS query, then at step **1522**, it is dropped. If, at step **1524**, the query is not a standard query, such as a DNS STATUS (a status lookup) or IQUERY (inverse DNS), or the class of the DNS query indicates an Internet (IN) query, or if the TYPE value of the request is a pointer (PTR) or host address (A), then, a "Not implemented" DNS response **1530** is sent over the virtual link to the Member Agent **565**.

At step **1540**, the VCN checks to see if the source IP address is for a member of the VCN. If the source IP address is not for a member of the VCN, the virtual IP look up fails or the type PTR query does not match, a "server failed" response **1545** is returned. At step **1550**, if there is no DNS Question section or there is another type of format error with the packet, a "format error" response **1555** is sent. The VCN determines whether the member has joined the VCN, at step **1560**. If not, a name error response is sent at **1565**.

If the name is a successful lookup (step **1570**), then the VCN Manager will send a DNS Response Packet **1575** to the member **565**. The response includes the following information: the target member FQDN; the target member virtual IP address; a source Route Director flag, the source member virtual IP address; the target member join time; the target member agent version; the target member private IP address; the target Route Director public IP address; the target member NetBIOS name; the shared key, shared by the two members; a target Ticket length; a target member Ticket encrypted for target member only and containing a Ticket issue time, Ticket expiration time, and shared key; the target member virtual IP address, the source member virtual IP address, the source member private IP address; the source Route Director public IP address, the source member FQDN; and padding (to obtain a multiple of 16 octets). The Ticket provided by the DNS request is detailed further in the description of FIG. **16**B.

The target member's virtual IP address will be presented nsing an A-type resource record in the answer section of the normal DNS response packet. All the remaining information will be transferred using a TXT-type resource record in an additional section of the DNS Response.

Encapsulation

Traffic between Member Agents in the VCN is encapsulated using UDP encapsulation. Encapsulated traffic between members can carry any IP traffic from any standard IPv4 compliant application. However, one port is set aside in the virtual network at the application layer to establish a connection between two members in the community. In one embodiment, this is UDP port **500**, which is set aside for Internet Key Exchange (IKE), allowing negotiation of an IPsec tunnel between the two members.

When an application on a member device wishes to open a connection to a peer on a target member device, a protocol is followed for the establishment of the IPsec session between the two. Member Agents are configured to listen on the UDP tunneling port (which defaults to port **20202**) for virtual traffic. As an accepted procedure non-IPsec traffic on the virtual IKE port **500** is accepted and passed to an IKE and Security Policy Module to allow for the possibility of initiating, an IKE exchange and the establishment of an IPsec session between the two members.

IKE is fully described in RFC-2409. IKE provides a key exchange with a peer and creates a security association (SA) for the IPsec module. IKE access between peers occurs in two phases: phase 1 establishes a secure, authenticated, channel with which to communicate, and phase 2, which negotiates a Security Association on behalf of IPsec. Phase 1 is generally referred to as the ISAKMP Security Association (SA) and includes a "Main Mode" and "Aggressive Mode." In one implementation, Aggressive Mode is used for phase 1. One of the allowed phase 2 exchanges is "Quick Mode" and in one implementation, Quick Mode is used in the system for phase 2.

FIG. **16**B shows the aggressive mode IKE phase one exchange utilized in the present invention. FIG. **16**A shows the standard aggressive mode IKE phase one exchange for comparison. In these figures, in accordance with standard IKE parlance, one device is considered an exchange "initiator" and the other a "responder".

In general, in phase one of the IKE exchange, peers are authenticated, an IKE Security Association (SA) policy between peers is established, a Diffie-Hellman exchange is performed to produce matching shared secret keys and a secure tunnel to negotiate IKE phase two parameters is established.

In FIG. **16**A, an initiator exchanges a header (HDR), SA negotiation payload, Key Exchange (KE), nonce payload (Ni, where "i" indicates an "initiator" payload) and identity of the party (IDii). The key exchange payload contains the public information exchanged in a Diffie-Hellman exchange. The responder returns the HDR, SA, KE, a responder nonce payload (Nr), its identity (IDir) and the HASH responder (HASH_R) payload, which is generally a hash of the ID payload and is used to authenticate the exchange. The initiator returns the HDR and HASH initiator (HASH_I) payload, and the initial secure tunnel is established.

In accordance with the present invention, FIG. **16**B illustrates the use of an extension to aggressive mode exchange. This is performed by adding a ticket payload (TKT*) to distribute a shared-key to remote peers.

The Ticket is the means by which one Agent can identify whether another Agent is a trusted member of the virtual community. Essentially, the Ticket includes information identifying the initiating member to the receiving member.

The ticket is issued by the VCN Manager and encrypted for the receiving member with a member-server shared secret; only the receiving member can open it. The ticket contains a time-stamp, a sequence number and a shared-secret used for IPSEC between the two members. To communicate with the receiving member, the initiating member obtains the ticket from the VCN Manager (through, for example, the DNS sequence, described above) and passes it to the receiving member in a payload that can ride on an IKE packet. The receiving member receives the Ticket, decrypts the Ticket using the member-server shared secret, and uses the information in the Ticket to establish secure communication with the initiating member.

This payload, TKT, is formatted as shown in FIG. **17**. The packet **1700** contains an IP header **1710**, UDP header **1720**, System shim **1730**, and Virtual IKE Phase 1 UDP/IP packet **1740**. FIG. **18** illustrates the structure and data of an exemplary first packet **1740**. The IKE Ticket Payload in the first IKE packet contains information on the payload and the payload data, including the type of payload following next and the ticket payload data **1756**. The payload data **1750** includes the size, number and item list **1766**. The item list **1760** includes type, size and item information. The IKE ticket payload data **1740** contains the item types

The item types **1770** are shown in the last table of FIG. **18**: "My FQDN"—a null terminated FQDN in label dot format. (For example, a human readable FQDN "bob.system.com" is encoded as "bob.system.com\0x00.") My Ticket data which includes a Manager Current Time (UTC of Manager as known by initiator); and an Initiator Virtual IP (Obtained at Join time) Target Virtual IP (Obtained from Manager) and Padding. The Peer FQDN Format is a null terminated FQDN in label dot format. For example, a human readable FQDN "bob.system.com" is encoded as "bob.system.com\0x00". Finally, the Peer Ticket data includes: a Ticket Issue Time (UTC (seconds) on VCN Manager); a Ticket Expiration (UTC (seconds) for ticket expiration); a Shared Key used hy the two Members for IKE; a Target Virtual IP Address; the Initiator NAT Port; the Initiator Subnet; the Initiator Virtual IP Address; Initiator Private IP Address, the Initiator Public IP Address, the Initiator FQDN and padding.

The Diffie-Hellman key exchange protocol is utilized in the Internet Key Exchange (IKE) protocol that precedes IPsec. The prime and generator value are taken from a well-known Internet Draft entitled, "More Diffie-Hellman groups for IKE," Kivinen et al., IP Security Protocol Working Group (IPSE) Internal Draft, Dec. 13, 2001, for proposed use within the Internet Key Exchange (IKE) protocol.

Administrative Functions

The system can simulate pings to any of the Route Directors (NRD or PRD). This ping is sent inside a packet generated from an application used to trouble-shoot the virtual network by touching the Route Directors and insuring that they are alive.

An exemplary ping process is illustrated in FIG. **19**. As shown therein a pinging application **1902** at step **1904** sends a ping request packet **1906** to the Route Director **560**. The Route Director receives the ping at **1910** and generates a response at step **1912**. The ping response packet **1914** is returned to the application **902** at step **1916**.

The ping request packet is sent and returned on the default tunneling UDP port (which in FIG. **5**B is UDP Port **20202**). The Ping Request **1906** packet is formatted as shown in FIG. **19**, with the content of the shim and the ping packets exploded in further detail. In the shim **1930**, the source and destination Route Director public IP addresses (gIP) and private IP addresses (pIP) are all set to 0. In the system ping field **1960**, the ping type field may be a ping request or a ping response. The Sequence field in the response is set to the same value as the Sequence field in the request packet.

Another function which may be performed is an Agent Query. FIG. **20** illustrates a query request from a Member Agent requiring system/status information of another member. The first Member Agent **565** at step **1802** will send a Query Request Packet **1810** to the VCN Manager **510**. The Packet contains definitions for the Maximum Number of Records to return, a status Mask indicating whether the members are registered and/or joined, a platform Mask, indicating the platform (desktop, server, laptop, mail server, etc) of the member, the FQDN Length, FQDN VCN Offset, Search

String Length, Member FQDN and a Search String for pattern matching. This packet is sent over the IPsec tunnel between the VCN Manager and the Member Agent.

If the packet is abnormal it is dropped at step **2012** if there is an error in the query authentication file or the member is not joined, NACK **2016** is sent in step **2014**. If the packet is not abnormal, no error is present, the member passes authentication and was joined. then the VCN Manager sends a query acknowledgement Packet **2030** to the member. The packet payload includes a number of records with the following fields: the status of the member, the platform type of the member, and the member's FQDN String. Note that the FQDN is null-terminated and consistent with the FQDN in DNS format definitions. Here, a human readable FQDN "www.abcdefg.com" is encoded as "www.abcdefg.com\0x00".

Each joined member will periodically send a heartbeat packet to the VCN Manager so that the VCN Manager can determine if the member is alive. In addition, the member's heartbeat packet is used to determine how long the member is actually joined. This information can be used to allow a provider of the infrastructure for the system to generate revenue from users on a per-use time basis. Conversely, the VCN Manager periodically sends its heartbeat packet to joined members so that the joined members can know if the Manager is alive. This can he used hy the memher to determine if it should switch to a backup VCN Manager. Heartbeat packets are sent inside the system tunnel on the default tunneling port (UDP port **20202**) and are IPsec protected.

Route Directors

Route directors allow communication to a member that is in a private network. The PRD resides within a private network, behind the NAT device. The NRD resides on the public side of the NAT device. The NAT device can be a Network Address Port Translation (NAPT) NAT device or a basic NAT where only addresses are translated.

Note that devices with pnhlic addresses do not require Route Directors (RDs). In the context of FIG. **5B**, devices M_A and M_E do not require either a PRD or NRD, since they reside in the public address space. Likewise, M_X does not require the PRD for its domain **540**, since it has a public address (or is statically mapped to a public address at the NAT device **515**).

The NRD implements a NAT traversal architecture which allows System packets to enter and exit a private network. The NRD maintains persistent connections/sessions with members that are behind NAT devices. Member Agents initiate a TCP or UDP persistent connection/session with the NRD and use keep-alive messages to ensure that the NAT device does not drop the member's connection/session. The use of TCP or UDP is based on a bit set by the VCN Manager in the INIT ACK packet of the Join Protocol. Communication to a member uses NRD tunnels between the NRD and the Memher Agent through the persistent connection/session. More information about a suitahle NAT traversal architecture is found in U.S. Pat. No. 7,139,828 and U.S. patent application Ser. No. 10/233,288, "Communicating With An Entity Inside a Private Network Using an Existing Connection to Initiate Communication," both of which are incorporated herein by reference.

When a member behind NAT attempts to join a virtual network by contacting the VCN Manager as discussed above, the VCN Manager will detect the presence of the NAT device, direct the member to a specific NRD and indicate the use of TCP or UDP. The presence of the NAT device must be detected during the initialize Init message portion of the join seqnence so the VCN Manager can inform the memher that it needs to setup a session with the assigned NRD prior to the Join message seqnence.

In one embodiment, the NRD uses a pseudo address. The pseudo address is different than the virtual address and is used solely for NRD routing. The pseudo address assigned by the NRD will allow the NRD to map a packet to the member's post-NAT IP address and UDP port.

The process for establishing a session with a NRD and obtaining an address therefrom is shown in FIG. **21**. Initially (as described in FIG. **13**), a member behind a firewall will send an init request **1304** to VCN Manager **510**. In addition to the functions performed with respect to step **1306**, **1308**, and **1311** (of FIG. **13**), the VCN Manager will detect that the member is behind a NAT device and whether it is served by a PRD in step **2120**.

The detection of a NAT device is accomplished using a field with the member's local IP address in the Init packet sent to the VCN Manager. The VCN Manager detects the fact that Agent **565** is behind a NAT device by comparing the member's private IP address in the INIT message payload with the source address in the TCP/IP headers. If the addresses differ, then a NAT device is present. At step **2120**, the VCN Manager must next check if the member's NAT device is associated with a known PRD (Premises Route Director). If no PRD is found, then the VCN Manager will check if the member can nse a known NRD. If an NRD is found then the INIT ACK **1314'** will indicate that the member must establish a session with the NRD prior to joining the VCN. If the NRD can support TCP tunneling, the INIT ACK will also indicate to the member to start a TCP connection rather than a UDP connection. If neither a PRD nor an NRD is found for the private member, an Init NACK will be returned. The VCN Manager will find an available NRD and send an INIT ACK **1314'** with the NRD info data contained therein. The contents of an INIT ACK packet **1314** are discussed above with respect to FIG. **13**.

At step **2132**, the member will seek to establish a session with the NRD and will send address request **2130** to the NRD. The memher sends the Address Request Packet **2130** to the NRD. The packet includes an IP Header, UDP Header or TCP header, and Shim. In this case, the shim includes the NRD's public address. At step **2135**, the NRD assigns the member a pseudo address. This is used as the member's private address in the Shim when external members send packets to the NRD for forwarding to the private member. The NRD will store the association of the pseudo address with the Member's NAT device public address and port number. When other members of the VCN perform a DNS request on the member behind the NRD, as part of the DNS response, they will receive the public address of the NRD and they will receive the pseudo address as the private address for the member behind the NRD. When sending a communication to the member behind the NRD, the outer packet will be addressed to the public address of the NRD. The NRD will access the shim to identify the pseudo address. The NRD uses the pseudo address as a handle to the persistent connection/session when sending packets through a NAT to the member. Once identifying the appropriate persistent connection/session, the shim and virtual packet are encapsulated and sent to the destination, via the NAT device, using the identified persistent connection/session. When the NAT device receives the message, it will do the address and port translation, and forward the message to the member agent's real local address and port on the private network.

In one aspect, the pseudo address comprises portions of the public IP address space in IP version 4 that had been reserved for special purposes. This ensures that no machine within a private realm will have the same pseudo IP address as the private address of a machine in any separate and distinct

private realm. In order to prevent this from happening, the system of the present invention uses addresses that are otherwise not used or reserved. Examples include the 0.0.0.0, the 10.0.0.0, 14.0.0.0, 127.0.0.0, 169.2454.0.0, 172.16.0.0 and the like.

The NRD provides the pseudo address to the Agent **565** in a NAT Traversal Address Response Packet **2140**. The packet includes a shim having an indicator that the response is a pseudo address response, as well as the source Route Director public IP address and Destination Route Director public IP address, (which is set equal to the NRD address), the Source member private IP address (0) and the Destination member private IP address, which is the Virtual IP. Hence all communications for the Member Agent will be routed to the NRD **520**. After acquiring the pseudo address from the NRD, the member designates that pseudo address to the VCN Manager as its local address in Join packet **1318**.

Note that there is an extra packet exchange **2145**, **2150** when establishing a TCP connection that is not required when establishing a UDP connection with the NRD. This packet is the NRD Init Request Packet **2145**. The previous TCP session for the Address Request and Address Response must be closed and a new TCP session opened which will remain open for the duration of the tunnel session. The member sends the Init Request message to the NRD as the first message in this TCP session. This message only has a TCP header and System Shim preamble, and has no data following the Shim.

After receiving the pseudo address, the join process completes with the join request packet **1318**, and join ack packets **1328**. After the join processing is complete, TCP/UDP encapsulated traffic flows between the member and the NRD through the NAT. The member is now ready to establish connections with other members.

When outbound System traffic from a member behind a NAT device to the NRD is not frequent enough to keep the NAT device's mappings active, the member may to send keep alive messages to the NRD's TCP port **80** or UDP encapsulation port to ensure that the NAT device does not drop the TCP/UDP encapsulation session. The member sends this message to the NRD to ensure that the NAT device does not drop the TCP/UDP port mapping. The keep-alive messages do not need to be sent when other messages were sent out during the keep-alive interval.

The member sends this NAT Traversal Leave Packet message to the NRD to release the session and pseudo address when the member is leaving the VCN. The NAT traversal switch will verify that the receive-from socket address this message came from matches the lookup table entry before deleting the member's address.

Group Agent

For some devices, member client software cannot be installed on the device or it is not desirable to install member client software on the device. For example, a printer or other networked devices may not be able to load software. For various reasons, some entities may not desire to add network software onto their machines. Additionally, some devices may use operating systems that do not support running the member agent software. For those devices that cannot or choose not to use member agent software, a Group Agent can be used. The Group Agent acts as a proxy for one or more members of a VCN without requiring installation of member agent software on the client devices. Thus, a device can become a member of a VCN without changing any of the software on the device by using the Group Agent.

FIG. **22** is a block diagram depicting various components of the present invention utilizing a Group Agent. Note that some of the members of a VCN can use a Group Agent while other members do not use a Group Agent. FIG. **22** shows ten devices M_1-M_{10}. Devices M_1, M_2, M_3, M_4 and M_{10} are devices that are participating in the VCN without using member agent software. Rather, they will use a Group Agent. Devices M_5, M_6, M_7, M_8 and M_9 are devices which include member agent software and, therefore, do not need to use a Group Agent. FIG. **22** shows some of the many varieties of permutations of using Group Agents, Network Route Directors and Private Route Directors. Other permutations can also be used with the present invention. Also note that FIG. **22** is more of a structural view of additional components of the present invention, as compared to FIG. **5B** which is more of a symbolic/logical view.

FIG. **22** includes a first private network which connects to the Internet (or other network) via NAT device **2202**. In addition to NAT **2202**, the private network includes device M_1, device M_2 and Group Agent **2204**. In one embodiment, the Group Agent runs on the same machine as a Private Route Director. Devices M_1 and M_2 do not include agent software. Rather, they participate in the VCN using Group Agent **2204**.

A second private network allows devices to communicate to the Internet (or other network) via NAT device **2210**. That private network also includes Group Agent **2212**, device M_3 and device M_4. Note that Gronp Agent **2212** does not include a Private Route Director. Thus, for devices M_3 and M_4 to be reached by other members of the VCN, communication is performed via Network Route Director **520**. In one embodiment, each of the private networks are different physical address realms. That is each uses a different set of private IP addresses. The present invention will also work if the private networks have overlapping addresses. That is, one or more private IP addresses are used by more than one private network involved in a VCN.

A third private network, which includes devices M_5 and M_6, provides for communication on the Internet via NAT device **2220**. A fourth private network, which includes devices M_7 and M_8, allows its components to communicate on the Internet (or other network) via NAT device **2230**. This fourth private network includes Private Route Director **2232**. Because devices M_7 and M_8 include member agent software, there is no need for a Group Agent on this network. Device M_9 has a public IP address and includes member agent software; therefore, it communicates and participates in the VCN as described above. Device M_{10} has a public IP address; however, device M_{10} does not include member agent software. For device M_{10} to participate in the VCN, it must make use of Group Agent **2234**, which has a public IP address.

In one embodiment, a Group Agent includes software running on a computing device, including (but not limited to) a server, router, personal computer, minicomputer, mainframe, mobile computing device, or other suitable computing device. In other embodiments, the Group Agent, or any other of the software components described above, can be performed by its special purpose computing device.

A Group Agent acts as a proxy for one or more members which do not have member agent software. For example, Group Agent **2204** is a proxy for devices M_1 and M_2; and Group Agent **2212** is a proxy for devices M_3 and M_4. Group Agent **2234** is a proxy for device M_{10}. Although FIG. **22** shows the Group Agents being proxies for one or two members, a Group Agent can be a proxy for more than two members.

Communication between two members of a VCN can pass through two NAT devices, one NAT device for each member. For example, communication between device M_1 and device M_4 will pass through NAT device **2202** and NAT device **2210**. Additionally, communication between device M_1 and another

entity in a private network configured like the private network of device M_1 will require communication to pass through two NAT devices.

Note that a single Group Agent can participate in more than one VCN. For example, Group Agent **2204** can be used to allow device M_1 participate in a first VCN and concurrently (for all or part of the time) allow device M_2 to participate in a second VCN. Because there can be multiple virtual community networks, the VCN Manager is able to create and maintain, the multiple virtual community networks. As described herein, the VCN Manager identifies which entities can communicate on each VCN hy maintaining a list of domain names for each VCN. For example, one list may include the domain names for devices M_1-M_{10}.

The Group Agent requires initialization so it may know which members it is a proxy for. Group Agent initialization cannot occur until after the Group Agent has joined the VCN Manager as a member. The join prior to Group Agent initialization is for a pseudo-member so the proxy initialization messages can use virtual IP addresses and the tunneling protocols described above to travel on an IPsec tunnel between VCN Manager **510** and the particular Group Agent. Separate member specific tunnels will be created when the Group Agent later joins for the proxied members. The Group Agent join will require the Group Agent to be registered with the VCN Manager. In one embodiment, this registration will be done during the installation of the Group Agent.

FIG. **23** provides a flowchart describing one embodiment of the process for Group Agent initialization. In step **2302**, the Group Agent joins as a pseudo-member. This process of step **2302** is performed as described above. In step **2304**, the Group Agent will send an initialization request to the VCN Manager. The initialization request is a packet that includes the fully qualified domain name for the Group Agent, a packet version indication, a packet type indicating that it is an initialization request, a packet length, and an authentication code. If the received initialization request is abnormal (step **2306**), then the initialization request is dropped in step **2308**. If the packet was normal but authentication failed (step **2312**), then the VCN Manager sends a NACK to the Group Agent in step **2314**. If authentication was successful and the initialization request was normal, then the VCN Manager sends an acknowledgement to the Group Agent in step **2320**.

After completion of step **2320**, the Group Agent is initialized and now must join each of the members it is proxying. To do so, the Group Agent will perform a loop where each iteration will include joining for one of the members that is being proxied. In step **2322**, it is determined whether there are any more members being proxied that have to be joined. If there are more members to join, then the Group Agent will join for one member being proxied in step **2324** and the method will loop back to step **2322**. When there are no more proxied members to be joined, the process of FIG. **23** is complete (step **2330**). The process of joining for a proxy member is the same as the process of joining described above; however, the process is performed for the member by the Group Agent rather than by the member agent. The virtual IP address received by the Group Agent is for the member being proxied. The Group Agent stores that virtual IP address in a data structure for the member. In one embodiment, there is a separate data structure for each member being proxied. In another embodiment, there is one data structure which has separate records for each member being proxied. This data stored will include the member's virtual IP address and private address in the local LAN, as well as other information that will he described below.

The acknowledgement sent from the VCN Manager to the Group Agent in step **2320** contains all of the member information required so the Group Agent can send the appropriate join requests for each member being proxied. The following information is in the acknowledgement sent from the VCN Manager to the Group Agent: packet version indicating the version of the header, packet type indicating that it is a acknowledgement, packet length, authentication code, subnet IP address, subnet prefix, public IP address of the Private Route Director (when the Group Agent also includes a Private Route Director), Private Route Director ping flag (1 if PRD responds to pings), the number of members being proxied, the number of permanent connections from proxied members to other members that the proxy must make, the member record list and the connect record list. The member record list is a set of records for each member being proxied. The following information is stored in each record: member password (password SHA1 digest), member's local private IP address, the length of the member's fully qualified domain name, the member's fully qualified domain name, offset to the VCN name, authentication type (0=preshared 1=certificate), time stamp indicating when the token key was created, token length in bytes, token key (member shared secret with VCN Manager), HA version number, number of HA records, HA record list and authentication key (generated by server for the proxy). Each HA record in the HA record list includes a VCN Manager IP address for the next VCN Manager, a join port for the next VCN Manager and a service port for the next VCN Manager in case the current VCN Manager goes down. The connect record list includes the following three fields: proxy member index (zero based index into member list), DNS request length and a DNS request.

Once the Group Agent joins for all of its members, then any of its members can receive communication from other members of the VCN or can initiate communication to other members in the VCN. Members that are being proxied by a Group Agent can communicate with other members being proxied by the Group Agent, with other members proxied by a different Group Agent (regardless of whether they are in a private network or available on the public Internet), and members that do not use a Group Agent (regardless of whether those other members are in a private network or available on the Internet with a public IP address), as long as they are all members of the same VCN. From the point of view of an application on a member being proxied by the Group Agent, the VCN appears as a local subnet (or LAN) and all of the members of the VCN appear to be on the local subnet (or LAN). However, the VCN is not a local subnet (or LAN); rather it is a virtual subnet (or LAN). Each of the members of the VCN will have a Virtual IP Address on the virtual subnet.

Because members of a VCN register with the VCN Manager, the VCN Manager will know how to find the members (e.g. it will know its public and private addresses). Thus, a Group Agent acting as a proxy for a first member will be able to act as an intermediary for that first member when talking to a second member of a VCN even if the second member moves to a different or new private network and/or changes its IP address. That is, when the second member makes the move or change, the second member will so inform the VCN Manager. The VCN Manager will inform the Group Agent of the change so that the Group Agent can continue to act as an intermediary between the first member and the group member. More information about communicating with mobile entities can be found in U.S. Pat. No. 7,139,828; U.S. patent application Ser. No. 10/161,573, "Creating A Public Identity For An Entity On A Network," filed on Jun. 3, 2002; and U.S. patent application Ser. No. 10/233,288, "Communicating With An Entity

Inside A Private Network Using An Existing Connection To Initiate Communication," filed on Aug. 30, 2002, all three applications are incorporated herein by reference in their entirety.

FIG. **24** is a flowchart describing one embodiment of a process for initiating communication with a member that is being proxied by a Group Agent. In FIG. **24**, the communication is being initiated by a member that is not being proxied by a Group Agent. That is, the member initiating communication is a member that has agent software loaded on it. That member is initiating communication with a member that does not have agent software. Prior to the process of FIG. **24** being performed, the Group Agent has joined the member into the VCN and the member initiating communication has already joined the VCN. For example purposes, looking at FIG. **22**, the process of FIG. **24** can be performed by M_5, M_6, M_7, M_8 or M_9 initiating communication with any of devices M_1, M_2, M_3, M_4 or M_{10}. Assume, for example purposes, that device M_9 is initiating communication with device M_1. The destination device is also assumed to be served by a Private Route Director.

In step **2402**, an application on the source device (e.g., device M_9) is intending to send a message to an application on the destination device (e.g., device M_1). In step **2404**, the application on the source device sends a DNS request to the VCN Manager using the domain name of the destination. For example, the application on M_9 will send a DNS request using the domain name for M_1. In step **2406**, the VCN Manager returns a response to the DNS request. This response includes the public IP address for private Route Director **2204**, the private IP address for member M_1 and the virtual IP address for member M_1. In some embodiments, the DNS response also includes a token key (as described above). The Agent on the source device (e.g., M_9) stores the information it received from the VCN Manager. In step **2410**, the Agent on the source device returns the virtual IP address for the destination to the application which initiated the DNS request. In step **2412**, the application on the source device initiates the sending of a message to M_1 using the virtual IP address. That is, a virtual IP packet is created where the source address is the virtual IP address for the source machine (M_9) and the destination address in the virtual IP packet is the virtual IP address for the destination device (device M_1). The virtual IP packet is created in step **2414** and subject to IPsec (or other security means). In step **2416**, the virtual IP packet is encapsulated. Encapsulation includes adding a shim, a UDP header and an IP header, all as described above. The shim includes the public IP address for the Private Route Director associated with the destination member (e.g., PRD **2204**) and the private IP address for destination (e.g. member M_1). If the source, the member initiating communication was in a private network, then the shim would also include the public IP address for the Route Director associated with the source and the private IP address for the source. In step **2418**, the encapsulated packet is sent to the NAT for the destination's private network. That is, in the example above, the newly created packet is sent to NAT **2202** via the Internet (or other network). In step **2420**, the encapsulated packet is sent from the NAT (e.g., NAT **2202**) to the Route Director for the destination (e.g., PRD **2204**).

In step **2422** of FIG. **24**, the Route Director removes the virtual IP packet and the shim from the encapsulation and presents both the virtual IP address and the shim to the Group Agent (e.g., Group Agent **2204**). The Group Agent stores the information from the shim, as described above with respect to the member agent software. In one embodiment, the Group Agent includes the necessary logic to received the communication so that no route director is necessary. In step **2426**, the Group Agent extracts the virtual IP packet from IPsec. In step **2428**, the Group Agent chooses a private IP address for the source entity. In the above example, the source entity is device M_9. Group Agent **2204** will pick a private IP address that is routable in the private network associated with device M_1 and NAT **2202**. This private address will be used by device M_1 to identify M_9. In step **2430**, the Group Agent will change the source address in the virtual packet. That is, the virtual packet originally had a source address equal to the virtual IP address for the source device (e.g., M_g) and a destination address equal to the virtual IP address for the destination device (e.g., M_1). In step **2430**, the source address in the virtual IP packet is changed to be equal to the private IP address chosen by the Group Agent for M_9 in step **2428**. In step **2432**, the Group Agent changes the destination address in the virtual IP packet to be equal to the private IP address in the local LAN for M_1. In step **2434**, the packet is sent by the Group Agent to the destination machine (e.g., sent to M_1).

The above discussion of FIG. **24** was made with respect to the example that the communication has been initiated by device M_9 which is a member having a public IP address and member agent software. The process of FIG. **24** can also be performed by a member which does not have a public IP address, including members using a Private Route Director and/or a Network Route Director. When the process of FIG. **24** is being performed by members using Route Directors, the shim that is added to the encapsulated packet in step **2416** includes the private IP address for the member and the public IP address for the Route Director. The example used in discussing FIG. **24** also assumes that the destination was a device in a private network where the private network included a Group Agent and a Private Route Director. The process of FIG. **24** can also be adapted to work with a member using a Group Agent where the member has a public IP address and/or a member in a private network that uses a Network Route Director.

When sending communication to an entity with a public IP address that uses a Group Agent, the shim will include the public IP address for the Group Agent and the public IP address for the member in step **2416**. The packet will not be sent to a NAT or to a Route Director. Rather, the packet will be sent directly to the Group Agent. The Group Agent will access the virtual IP packet in step **2426**. Rather than choosing a private IP address to identify the source, the Group Agent will choose a public IP address for the destination to use to refer to the source. The virtual IP packet will be changed so that the source address is equal to the public IP address chosen by the Group Agent to represent the source and the destination address will become the public IP address for the destination. The virtual IP packet (which is no longer virtual) will be sent to the destination.

If the destination member participates in a VCN using a Network Route Director (e.g., device M_3 using NRD **520**), then the encapsulated packet is sent to the Network Route Director in step **2418**. The Network Route Director will communicate the shim and virtual IP packet to the Group Agent (e.g., Group Agent **2212**) via a persistent connection as described above in FIG. **7**, steps **673-675, 677**, except that the packet is forwarded to the Group Agent rather than the NAT device. The Group Agent will then perform steps **2424-2434**, as described above.

FIG. **25** is a flowchart describing one embodiment of a process for the destination device responding to the initiation of communication from the source device. In the example discussed above, this process would include device M_1 responding to device M_9. In step **2502**, the application on

device M_1 attempts to send a communication. A packet is then created using the private addresses. The packet would include a source address equal to the private IP address in the LAN for device M_1. The destination address would be equal to the private IP address in the LAN that is used to identify device M_9. That packet is sent to the Group Agent in step **2504**. In step **2506**, the Group Agent changes the packet by replacing the private addresses with virtual addresses. The source address is replaced with the virtual IP address in the VCN used to identify device M_1. The destination address in the packet is replaced with the virtual IP address in the VCN used to identify device M_9. In step **2508**, this packet is subject to IPsec, and encapsulated as described above.

In step **2512** of FIG. **25**, the Group Agent sends the packet. In the example above, the Group Agent would send the encapsulated packet to device M_9 using the public IP address for device M_9. If the Group Agent is sending the packet to a member that is in a private network, then the encapsulated packet would be sent to the Group Agent/Private Route Director for the member or to the Network Route Director for that member. If the responding device (e.g. M_1) is using a Network Route Director, then the Group Agent can still send the reply packet directly to the original source without going through the Network Route Director. If the replying device (e.g. M_1) has a puhlic IP address, then the packet sent to the Group Agent would include the public IP addresses for the responding device and the public IP address that the Group Agent told the replying device to use to identify the original source device. In one embodiment, when the member using the Group Agent has a public IP address, an IPsec tunnel can be created between the Group Agent and the member device.

FIG. **24** contemplates communication being initiated by a device that has member software loaded on it. FIG. **26**, on the other hand, describes a process that is performed when communication is initiated by a device that does not have member software and, therefore, nses Group Agent software. In step **2602**, the application on the initiating member will send a DNS request. This DNS request will he sent to the Group Agent. The Group Agent receives the DNS request in step **2604**. In step **2606**, the Group Agent sends its own DNS request for the same domain name to the VCN Manager. In step **2608**, the Group Agent receives a response from the VCN Manager. This response will include the virtual IP address for the target, the public IP address of the Route Director for the target (if any) and the private IP address for the target (if any). If the target has a public IP address, then the public IP address will be returned. In step **2610**, the Group Agent will choose a private IP address in the local LAN to be used to identify the target. The virtual IP address returned from the DNS request will be mapped to this private IP address in the local LAN. In step **2612**, the Group Agent will return that chosen private IP address to the application as a response to the application's DNS response. In step **2614**, the application will initiate the communication. In one embodiment, the process of **2614** includes performing the steps of FIG. **25**. Note that if the member who is initiating the communication in the process of FIG. **26** has a public IP address, rather than being in a private network, then in step **2610** the Group Agent will map the virtual IP address to a public IP address that the Group Agent and member will use to identify the target. It is this mapped public IP address that is returned to the application in response to the DNS request. The mapped public IP address is routable to the Group Agent.

Although the Group Agent is described above with respect to use with a VCN, the technology of the Group Agent is hroader than a VCN. Thus, the Gronp Agent can he used to allow entities to participate in other types of networks, communities, groups, organizations, communications, etc.

Note that in one embodiment, the member being serviced by the Group Agent must be in the same physical address realm as the Group Agent. In this manner, the Group Agent is used to bridge that physical address realm with the virtual space. The Group Agent contains the functionality to allow the member to participate in the virtual community; however, all the protocols of the virtual community terminate at the Group Agent. This way, the member receives a normal IP packet. From the point of view of the member, the Group Agent works like a router which connects the member to the subnet of virtual nodes.

The foregoing detailed description of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. For example, any number of VCN Managers may be used. Any combination of NRDs and PRDs may be used to improve network efficiency. Any combination of Member Agents and Group Agents may be used, and the Virtual Community may be of any size. Additionally, while the above description provided an example using the protocols and addressing currently used on the Internet, the present invention can be used with other protocols and addressing schemes. The described embodiments were chosen in order to best explain the principles of the invention and its practical application to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the claims appended hereto.

We claim:

1. A virtual network system, comprising:

a virtual network manager implemented with a first device memory and a first device processor of a first computing device, the virtual network manager configured to register devices in a virtual network that is defined hy a domain name, each device in the virtual network being identified to the other devices by a virtual network address that is unique for each device and not directly routable via a public network, the virtual network manager further configured to distribute a virtual network address to a device when the device is registered in the virtual network;

a route director implemented with a second device memory and a second device processor of a second computing device, the route director configured to communicate data between the devices that are registered in the virtual network, the data being communicated as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device; and

the virtual network manager further configured to receive a DNS request from the source device, and return a public network address of the route director, a private network address for the destination device, and the second virtual network address that corresponds to the destination device.

2. The system of claim **1** wherein each of the devices communicate with the virtual network manager and the other devices in the virtual network via an associated agent.

3. The system of claim **2** wherein the associated agent is installed on a proxy device which is a proxy agent for one or

more of the devices in the virtual network with respect to the virtual network manager and the route director.

4. The system of claim **2** wherein the virtual network manager is further configured to:

receive a request from the agent associated with a device in a private network to register the device in the virtual network; and

detect a presence of a NAT device via which the request is routed from the agent to the virtual network manager.

5. The system of claim **4** wherein the virtual network manager is further configured to receive the request from the agent as a message, and detect the presence of the NAT device by comparing a field in a payload of the message with a source address in a header of the message.

6. The system of claim **1** wherein each of the devices include an agent configured to communicate with the virtual network manager and agents of the other devices in the virtual network.

7. The system of claim **1** wherein the virtual network manager is coupled to the public network and has an associated public network address.

8. The system of claim **1** wherein the route director is further configured to receive the encapsulated packets when routed to a public network address corresponding to the route director.

9. The system of claim **1** wherein each of the devices in the virtual network are further identified by at least one physical network address.

10. The system of claim **9** wherein the physical network addresses that are associated with the devices in the virtual network are dynamic.

11. The system of claim **9** wherein the physical network addresses that are associated with the devices in the virtual network are static.

12. The system of claim **9** wherein the physical network addresses that are associated with the devices in the virtual network are private network addresses, and wherein the virtual network addresses are unique in the virtual network so as not to conflict with the private network addresses.

13. The system of claim **9** wherein the source device is coupled to a first private network and accesses a public network via a first NAT device configured to transmit the encapsulated packets, an encapsulated packet further including the physical network address of the source device as a private network address in the first private network.

14. The system of claim **13** wherein the physical network address of the source device is dynamic.

15. The system of claim **13** wherein the physical network address of the source device is static.

16. The system of claim **13** wherein the destination device is coupled to a second private network and accesses the public network via a second NAT device, the encapsulated packet further including the physical network address of the destination device as a private network address in the second private network.

17. The system of claim **16** wherein the physical network address of the destination device is dynamic.

18. The system of claim **16** wherein the physical network address of the destination device is static.

19. The system of claim **16** wherein said first private network and said second private network share at least one network address.

20. The system of claim **1** wherein the route director is further configured to:

provide a device-specific pseudo address assignment for the device in the virtual network when the device communicates with the route director via a NAT device; and

store an association of the device-specific pseudo address with a public network address of the NAT device and a port number of the NAT device.

21. The system of claim **1** wherein the route director includes a translator for virtual network address information for a device in the virtual network that is implemented in a private network.

22. The system of claim **1** wherein the virtual network manager is coupled to the public network and includes a public network address.

23. The system of claim **22** wherein the route director is coupled to the public network and includes a different public network address than the public network address of the virtual network manager.

24. The system of claim **22** wherein the route director is coupled to a private network and includes a private network address.

25. The system of claim **1** wherein the encapsulated packets further include virtual IP packets configured for communication of the data, the virtual IP packets being encrypted prior to being encapsulated.

26. The system of claim **25** wherein the virtual IP packets are encrypted using IPSEC.

27. The system of claim **25** wherein the virtual IP packets are encrypted using DES or triple DES.

28. The system of claim **1** wherein the virtual network manager includes a virtual community definition that is defined by the domain name, and includes one or more of the devices that are registered in the virtual network.

29. The system of claim **1** wherein the route director is a public route director in the public network, the system further comprising a private route director in a private network configured to enable access to devices of the private network that are also in the virtual network from devices of the public network that are also in the virtual network.

30. A virtual network manager, comprising:

a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;

a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to:

receive a registration request from an agent associated with a device;

distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and

a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.

31. The virtual network manager of claim **30** further comprising an additional network interface configured for data communication via a public network.

32. The virtual network manager of claim **31** wherein the network interface is a UDP port configured for data communication via the virtual network, and wherein the additional network interface is a TCP port configured for registration communications via the public network.

33. The virtual network manager of claim **30** wherein the network interface is a UDP port configured for data communication via the virtual network.

34. The virtual network manager of claim 30 wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network.

35. The virtual network manager of claim 30 further comprising a join module configured to receive a join request from the agent associated with the device to indicate that the device is connected for data communication within the virtual network, the join module further configured to receive a leave request from the agent associated with the device to indicate that the device will be disconnected from data communication within the virtual network.

36. The virtual network manager of claim 35 wherein the join module is further configured to provide virtual network addresses to the devices that are registered in the virtual network.

37. The virtual network manager of claim 35 wherein the join module is further configured to maintain data to associate a virtual network address with a device in the virtual network.

38. A virtual network system, comprising:

a computing device that includes at least a memory and a processor configured to implement a network manager of a virtual network that is defined by a public domain name, the network manager configured to distribute virtual network addresses to devices that register as members in the virtual network, each device in the virtual network being identified to the other devices by a virtual network address associated with the device;

a first virtual network agent associated with a first device that is registered as a member in the virtual network;

at least a second virtual network agent associated with at least a second device that is registered as a member in the virtual network;

a route director configured to route communications between the first device and the at least second device in the virtual network via the respective first and second virtual network agents, the communications configured for routing as encapsulated packets that include a first virtual network address that is not directly routable corresponding to the first device and a second virtual network address that is not directly routable corresponding to the at least second device; and

the network manager includes a DNS server configured to provide authoritative responses for DNS queries in the virtual network, the DNS server further configured to receive a DNS query from the first device and return a network address of the route director, a network address of the second device, and the virtual network address of the second device.

39. The system of claim 38 wherein the route director is a public network route director that includes a public network interface and the network address is a public network address by which the first and second virtual network agents communicate with the public network route director.

40. The system of claim 38 wherein the route director is a private route director that includes a private physical network interface and the network address is a private physical network address.

41. The system of claim 38 wherein the first virtual network agent is installed on the first device for data communication via the virtual network.

42. The system of claim 41 wherein the first device is in a private physical network, has an associated private network address, and has the associated virtual network address that is not directly routable by which the first device can be identified by the at least second virtual network agent from outside of the private physical network.

43. The system of claim 41 wherein the first device is coupled to a public physical network, has an associated public network address, and has the associated virtual network address by which the first device can be identified by the at least second virtual network agent.

44. The system of claim 38 wherein the first virtual network agent is a proxy agent for the first device with respect to the network manager and the route director.

45. The system of claim 38 wherein the first and second devices are configured to access the virtual network from separate private address physical realms.

46. The system of claim 38 wherein the network manager includes at least a first community definition and a second community definition, the first community definition being defined by the public domain name and includes one or more of the devices that are registered in the virtual network, and the second community definition being defined by a different public domain name and includes one or more different devices that are registered in the virtual network.

47. The system of claim 38 wherein the network manager includes a member authenticator configured to authenticate the devices that request to register with the network manager.

48. A computer-implemented method, comprising:

receiving registration requests from devices that request to be registered as members of a virtual network that is defined by a domain name having an associated public network address in a public network, each of the devices having an associated private network address;

distributing a virtual network address to a device to register the device as a member in the virtual network, each device in the virtual network being identified to the other devices by the virtual network address that is associated with the device;

routing communications between the devices that are registered in the virtual network, the communications being routed as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device; and

transmitting a response to a DNS request received from one of the devices that are the members in the virtual network, the response to the DNS request including a public network address of a route director that registers the devices, a public network address of the destination device, and the second virtual network address that corresponds to the destination device.

49. The method of claim 48 further comprising providing the devices in the virtual network with a communication agent.

50. The method of claim 49 wherein said providing the devices in the virtual network with a communication agent includes providing a proxy agent.

51. The method of claim 48 further comprising authenticating the devices as the members in the virtual network.

52. The method of claim 48 further comprising defining a member set of the virtual network that includes one or more of the devices, and assigning the domain name that defines the virtual network.

53. The method of claim 48 further comprising defining at least two member sets of the virtual network that each include one or more of the devices, the at least two member sets having at least one different device.

54. The method of claim 48 further comprising assigning the virtual network address to the device as an IPV4 compliant address.

55. The method of claim 54 wherein the IPV4 compliant address is non-routable.

56. The method of claim 48 further comprising routing network traffic via the public network from a first device having a public network address to a second device having a different public network address, the network traffic being routed as data packets having a source address which is the virtual network address of the first device and a destination address which is the virtual network address of the second device, the data packets being encapsulated to include a second source address which is a public network address of the first device and a second destination address which is the different public network address of the second device.

57. The method of claim 48 further comprising routing network traffic from a first device in a private physical network having a private network address to a second device having a public network address, the network traffic being routed as data packets having a source address which is the virtual network address of the first device, a destination address which is the virtual network address of the second device, and a shim which includes the private network address, the data packets being encapsulated to include a second destination address which is the public network address of the second device.

58. The method of claim 48 further comprising routing network traffic from a first device in a private physical network having a first private network address to a second device in a different private physical network having a second private network address, the network traffic being routed as encapsulated packets having a source address which is the virtual network address of the first device, a destination address which is the virtual network address of the second device, and a shim which includes the first and second private network addresses.

59. The method of claim 58 wherein the first private network address and the second private network address are identical.

60. The method of claim 48 further comprising:

receiving a join status request from a first device in the virtual network as a query to determine the status of a second device in the virtual network; and

responding to the join status request to indicate whether or not the second device is joined to the virtual network for data communication.

61. The method of claim 48 further comprising applying a group policy to the devices that are registered as the members of the virtual network.

62. One or more processor readable storage media devices comprising processor readable code that, if executed by a computer device, implements a virtual network manager to:

receive registration requests from devices that request to be registered as members of a virtual network that is defined by a domain name having an associated public network address in a public network, each of the devices having an associated private network address;

distribute a virtual network address to a device to register the device as a member in the virtual network, each device in the virtual network being identified to the other devices by the virtual network address that is associated with the device;

manage communications routed between the devices that are registered in the virtual network, the communications routed as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device; and

transmit a response to a DNS request received from one of the devices that are the members in the virtual network, the response to the DNS request including a public network address of the virtual network manager, a public network address of the destination device, and the second virtual network address that corresponds to the destination device.

63. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to provide the devices in the virtual network with a communication agent.

64. One or more processor readable storage media devices as recited in claim 63 wherein the virtual network manager provides the as a proxy agent.

65. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to define a member set of the virtual network that includes one or more of the devices, and the domain name that defines the virtual network.

66. One or more processor readable storage media devices as recited in claim 62 wherein the virtual network address includes a non-routable IPV4 compliant address.

67. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to route network traffic via the public network from a first device having a public network address to a second device having a different public network address.

68. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to route network traffic from a first device in a private physical network having a private network address to a second device having a public network address.

69. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to route network traffic from a first device in a private physical network having a first private network address to a second device in a different private physical network having a second private network address.

70. One or more processor readable storage media devices as recited in claim 69 wherein the network traffic is routed to the first or second device via a NAT device.

71. One or more processor readable storage media devices as recited in claim 69 wherein the first private network address and the second private network address are identical.

72. One or more processor readable storage media devices as recited in claim 67 wherein the network traffic is routed as encapsulated data packets.

73. One or more processor readable storage media devices as recited in claim 67 wherein the network traffic is routed as encrypted data traffic.

74. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to apply a group policy to the devices that are registered as the members of the virtual network.

75. A virtual network system, comprising:

a computing device that includes at least a memory and a processor configured to implement a virtual network manager having a network interface coupled to a virtual network, the virtual network manager including at least one virtual community definition that is defined by a domain name having an associated puhlic network

address and a user set of one or more devices that are registered in the virtual network, each device in the virtual network being identified to the other devices by a virtual network address that is associated with the device, the virtual network manager configured to exchange virtual network information with the one or more devices of the user set, the virtual network being accessible by devices in the user set and devices outside of the user set, and the virtual network manager further configured to receive a DNS request from a source device, and return a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device.

76. The system of claim **75** wherein the virtual network manager includes a member register module.

77. The system of claim **75** wherein the virtual network manager includes a member join module.

78. The system of claim **77** wherein the member join module provides a virtual network address to a device that is registered as a member of the network.

79. The system of claim **75** wherein the virtual network manager is further configured to maintain data on an association between at least one virtual network address with at least one device that is registered as a member of the network.

80. The system of claim **75** wherein the virtual network manager includes a DNS server for the virtual community network.

81. The system of claim **75** wherein the virtual network manager includes a NAT device detector for devices connecting with the virtual network manager behind a NAT device.

82. The system of claim **75** wherein the virtual network manager includes at least a second virtual community definition.

83. The system of claim **75** wherein the virtual network manager includes a member authenticator.

84. The system of claim **75** wherein the virtual network manager includes a DNS server configured to provide authoritative responses for DNS queries from devices in the virtual community.

85. The system of claim **75** further comprising at least one route director configured to communicate with the one or more devices in the user set.

86. The system of claim **75** wherein each device registered in the network is configured to communicate with the virtual network manager and other devices in the user set via at least one agent.

87. The system of claim **75** wherein the user set includes at least a first device and a second device, and wherein at least one of said first device and said second device is coupled to a first private network and accesses a public network via a NAT device.

88. The system of claim **87** wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

89. The system of claim **75** wherein communications between the one or more devices in the user set are encrypted.

90. The system of claim **89** wherein the virtual network manager is configured to provide a shared message to the one or more devices in the user set to establish encrypted communications.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 7,949,785 B2
APPLICATION NO.	: 10/403818
DATED	: May 24, 2011
INVENTOR(S)	: Alkhatib 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 3, item (56), under "Other Publications", in Column 1, Line 11, delete "Nelowrks." and insert -- Networks. --.

Title Page 3, item (56), under "Other Publications", in Column 2, Line 22, delete "Infrastucture" and insert -- Infrastructure --.

Column 40, line 15, in Claim 64, delete "the" and insert -- the communication agent --.

Signed and Sealed this
First Day of November, 2011

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

PTO/SB/57 (11-23)
Approved for use through 11/30/2024. OMB 0651-0064
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.

(Also referred to as FORM PTO-1465)

REQUEST FOR *EX PARTE* REEXAMINATION TRANSMITTAL FORM

Address to:
Mail Stop *Ex Parte* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attorney Docket No.: IVI785

Date: May 22, 2024

1. ■ This is a request for *ex parte* reexamination pursuant to 37 CFR 1.510 of patent number 7,949,785 issued May, 24, 2011. The request is made by:
   ☐ patent owner. ■ third party requester.

2. ■ The name and address of the person requesting reexamination is:
   Unified Patents, LLC
   4445 Willard Ave., Suite 600
   Chevy Chase, MD 20815

3. Requester ☐ asserts small entity status (37 CFR 1.27) or ☐ certifies micro entity status (37 CFR 1.29). Only a patent owner requester can certify micro entity status. Form PTO/SB/15A or B must be attached to certify micro entity status.

4. This request is accompanied by payment of the reexamination fee as set forth in:
   ■ 37 CFR 1.20(c)(2); **or**
   ☐ 37 CFR 1.20(c)(1). **In checking this box for payment of the fee set forth in 37 CFR 1.20(c)(1), requester asserts that this request has forty (40) or fewer pages and complies with all other requirements of 37 CFR 1.20(c)(1).**

   Payment of the reexamination fee is made by the method set forth below.
   a. ☐ A check in the amount of $_____ is enclosed to cover the reexamination fee;
   b. ☐ The Director is hereby authorized to charge the reexamination fee to Deposit Account No. _____;
   c. ☐ Payment by credit card. Form PTO-2038 is attached; **or**
   d. ■ Payment made via USPTO patent electronic filing system.

   ■ In addition, the Director is hereby authorized to charge any fee deficiencies to Deposit Account No. 50-6990.

5. ■ Any refund should be made by ☐ check or ■ credit to Deposit Account No. 50-6990. 37 CFR 1.26(c). If payment is made by credit card, refund must be to credit card account.

6. ■ A copy of the patent to be reexamined having a double column format on one side of a separate paper is enclosed. 37 CFR 1.510(b)(4).

7. ☐ CD-ROM or CD-R in duplicate, Computer Program (Appendix) or large table
   ☐ Landscape Table on CD

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0064. Public burden for this form is estimated to average 18 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, 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.

8. ☐ Nucleotide and/or Amino Acid Sequence Submission
If applicable, items a. – c. are required.
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM (2 copies) or CD-R (2 copies) **or**
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies.

9. ■ A copy of any disclaimer, certificate of correction or reexamination certificate issued in the patent is included.

10. ■ Reexamination of claim(s) 30, 34 is requested.

11. ■ A copy of every patent or printed publication relied upon is submitted herewith including a listing thereof on Form PTO/SB/08, PTO-1449, or equivalent.

12. ☐ An English language translation of all necessary and pertinent non-English language patents and/or printed publications is attached.

13. ■ The attached detailed request includes at least the following items:
   a. A statement identifying each substantial new question of patentability based on prior patents and printed publications. 37 CFR 1.510(b)(1).
   b. An identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited art to every claim for which reexamination is requested. 37 CFR1.510(b)(2).

14. ☐ A proposed amendment is included (only where the patent owner is the requester). 37 CFR 1.510(e).

15. ■ It is certified that the statutory estoppel provisions of 35 U.S.C. 315(e)(1) or 35 U.S.C. 325(e)(1) do not prohibit requester from filing this *ex parte* reexamination request. 37 CFR 1.510(b)(6).

16. Service
   a. ■ It is certified that a copy of this request (if filed by other than the patent owner) has been served in its entirety on the patent owner as provided in 37 CFR 1.33(c).

      The name and address of the party served are:

      MCANDREWS HELD & MALLOY, LTD
      500 WEST MADISON STREET, SUITE 3400
      CHICAGO, IL 23446

      Date of Service: May 22, 2024

   OR

   b. ☐ A duplicate copy is enclosed since service on patent owner was not possible. An explanation of the efforts made to serve patent owner **is attached**. See MPEP 2220.

17. Correspondence Address: Direct all communication about the reexamination to:

☒ The address associated with Customer Number: 165774

OR

☐ Firm or Individual Name _____
(at the address identified below)

Address

Unified Patents, LLC, 4445 Willard Avenue, Suite 600

City	State	Zip
Chevy Chase	MD	20815

Country

United States

Telephone	Email
(202) 701-1850	jordan@unifiedpatents.com

18. ☒ The patent is currently the subject of the following concurrent proceeding(s):

a. ☐ Copending reissue Application No. _____

b. ☐ Copending reexamination Control No. _____

c. ☐ Copending Interference No. _____

d. ☒ Copending litigation styled:

See Attachment

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.

/Jordan M. Rossen/	May 22, 2024
Authorized Signature	Date
Jordan M. Rossen	74,064
Typed/Printed Name	Registration No.

☐ For Patent Owner Requester ☒ For Third Party Requester

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. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to:

1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;

2) a federal, state, local, or international agency, in response to its request;

3) a contractor of the USPTO having need for the information in order to perform a contract;

4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;

5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;

6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;

7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;

8) 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));

9) the Office of Personnel Management (OPM) for personnel research purposes; and

10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Co-pending Litigations

- *Intellectual Ventures I LLC et al v. JP Morgan Chase & Co.*, Case No. 2:23-cv-00523 (E.D. Tex. Nov. 15, 2023);
- *Intellectual Ventures I LLC et al v. Liberty Mutual Holding Company Inv. et al*, Case No. 2:23-cv-00525 (E.D. Tex. Nov. 15, 2023);
- *Intellectual Ventures I LLC et al v. Comerica Inc.*, Case No. 2:23-cv-00524 (E.D. Tex. Nov. 15, 2023);
- *Assurant v. Intellectual Ventures I LLC et al*, Case No. 1:24-cv-00344 (D. Del. Mar. 15, 2023).

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 2698

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
90/019,519	05/22/2024 RULE	709	3992	IVI785

APPLICANTS

INVENTORS

7949785, Residence Not Provided;
Unified Patents, LLC, Residence Not Provided;
Intellectual Ventures i LLC (Patent Owner), Wilmington, DE;
Unified Patents LLC (3rd Pty Req.), Chevy Chase, MD;
Hasan S. Alkhatib, Saratoga, CA;
Fouad A. Tobagi, Los Altos, CA;
Farid F. Elwailly, San Jose, CA;

**** CONTINUING DATA ***************************

This application is a REX of 10/403,818 03/31/2003 PAT 7949785
*

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

Foreign Priority claimed ❑ Yes ❑ No 35 USC 119(a-d) conditions met ❑ Yes ❑ No Verified and Acknowledged _____ Examiner's Signature	❑ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
				90	6

ADDRESS

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661
UNITED STATES

TITLE

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
0.00	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

BIB (Rev. 05/07).

Patent Assignment Abstract of Title

Total Assignments: 5

Application #: 10403818 **Filing Dt:** 03/31/2003 **Patent #:** 7949785 **Issue Dt:** 05/24/2011
PCT #: NONE **Intl Reg #:** **Publication #:** US20040249911 **Pub Dt:** 12/09/2004
Inventors: Hasan S. Alkhatib, Fouad A. Tobagi, Farid F. Elwailly
Title: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Assignment: 1

Reel/Frame: 014196 / 0265 **Received:** 06/25/2003 **Recorded:** 06/24/2003 **Mailed:** 12/16/2003 **Pages:** 18
Conveyance: SECURITY INTEREST (SEE DOCUMENT FOR DETAILS).
Assignor: IP DYNAMICS INC. **Exec Dt:** 05/12/2003
Assignee: DAVID SUN AND DIANA SUN
17150 NEW HOPE STREET, SUITE 503
FOUNTAIN VALLEY, CALIFORNIA 92708
Correspondent: VIERRA MAGEN MARCUS ET.AL.
BURT MAGEN
685 MARKET STREET, SUITE 540
SAN FRANCISCO, CA 94105

Assignment: 2

Reel/Frame: 014340 / 0968 **Received:** 08/06/2003 **Recorded:** 08/04/2003 **Mailed:** 02/18/2004 **Pages:** 5
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignors: ALKHATIB, HASAN S. **Exec Dt:** 07/14/2003
TOBAGI, FOUAD A. **Exec Dt:** 07/14/2003
ELWAILLY, FARID F. **Exec Dt:** 07/29/2003
Assignee: IP DYNAMICS, INC.
2880 STEVENS CREEK BOULEVARD
3RD FLOOR
SAN JOSE, CALIFORNIA 95128
Correspondent: VIERRA MAGEN MARCUS HARMON & DENIRO LLP
BURT MAGEN
685 MARKET STREET, SUITE 540
SAN FRANCISCO, CA 94105

Assignment: 3

Reel/Frame: 020393 / 0423 **Received:** 01/21/2008 **Recorded:** 01/21/2008 **Mailed:** 01/22/2008 **Pages:** 5
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignor: IP DYNAMICS, INC. **Exec Dt:** 01/07/2008
Assignee: INPRO NETWORK FACILITY, LLC
2711 CENTERVILLE ROAD, SUITE 400
WILMINGTON, DELAWARE 19808
Correspondent: SADLER, BREEN, MORASCH & COLBY, PS
422 W. RIVERSIDE AVE, SUTIE 424
SPOKANE, WA 99201

Assignment: 4

Reel/Frame: 037490 / 0592 **Received:** 01/14/2016 **Recorded:** 01/14/2016 **Mailed:** 01/15/2016 **Pages:** 17
Conveyance: MERGER (SEE DOCUMENT FOR DETAILS).
Assignor: INPRO NETWORK FACILITY, LLC **Exec Dt:** 08/12/2015
Assignee: F. POSZAT HU, L.L.C.
2711 CENTERVILLE ROAD
SUITE 400
WILMINGTON, DELAWARE 19808
Correspondent: MCANDREWS HELD & MALLOY LTD.
500 W. MADISON STREET
34TH FLOOR
CHICAGO, IL 60661

Assignment: 5

Reel/Frame: 065469 / 0182 **Received:** 11/06/2023 **Recorded:** 11/06/2023 **Mailed:** 11/07/2023 **Pages:** 4
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: F. POSZAT HU, L.L.C. **Exec Dt:** 11/02/2023

Assignee: INTELLECTUAL VENTURES I LLC
251 LITTLE FALLS DRIVE
WILMINGTON, DELAWARE 19808

Correspondent: INTELLECTUAL VENTURES MANAGEMENT - IP LEGAL
3150 - 139TH AVE SE BUILDING 4
BELLEVUE, WA 98005

Search Results as of: 05/24/2024 10:16 AM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.6
Web interface last modified: Jun 26, 2017 v.2.6

UNITED STATES PATENT AND TRADEMARK OFFICE

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

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/019,519	05/22/2024	7949785

CONFIRMATION NO. 2698

REEXAM ASSIGNMENT NOTICE

23446
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

Date Mailed: 05/28/2024

NOTICE OF ASSIGNMENT OF REEXAMINATION REQUEST

The above-identified request for reexamination has been assigned to Art Unit 3992. All future correspondence to the proceeding should be identified by the control number listed above and directed to the assigned Art Unit.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or to all owners of record. (See 37 CFR 1.33(c)). If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned within the request to withdraw pursuant to Section 1.36.

NOTICE OF USPTO EX PARTE REEXAMINATION PATENT OWNER STATEMENT WAIVER PROGRAM

The USPTO has implemented a pilot program where, after a reexamination proceeding has been granted a filing date and before the examiner begins his or her review, the patent owner may orally waive the right to file a patent owner's statement. See *"Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings,"* 75 FR 47269 (August 5, 2010). One goal of the pilot program is to reduce the pendency of reexamination proceedings and improve the efficiency of the reexamination process.

Ordinarily when ex parte reexamination is ordered, the USPTO must wait until after the receipt of the patent owner's statement and the third party requester's reply, or after the expiration of the time period for filing the statement and reply (a period that can be as long as 5 to 6 months), before mailing a first determination of patentability. The USPTO's first determination of patentability is usually a first Office action on the merits or a Notice of Intent to Issue Reexamination Certificate (NIRC).

Under the pilot program, the patent owner's oral waiver allows the USPTO to act on the first determination of patentability immediately after determining that reexamination will be ordered, and in a suitable case issue the reexamination order and the first determination of patentability (which could be a NIRC if the claims under reexamination are confirmed) at the same time.

Benefits to the Patent Owner for participating in this pilot program include reduction in pendency.

To participate in this pilot program, Patent Owners may contact the USPTO's Central Reexamination Unit (CRU) at 571-272-7705. The USPTO will make the oral waiver of record in the reexamination file in an interview summary and a copy will be mailed to the patent owner and any third party requester.

cc: Third Party Requester(if any)
Unified Patents, LLC
4445 Willard Ave.
Suite 600
Chevy Chase, MARYLAND 20815

/rbell/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

UNITED STATES PATENT AND TRADEMARK OFFICE

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

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/019,519	05/22/2024	7949785

CONFIRMATION NO. 2698

REEXAMINATION REQUEST NOTICE

Unified Patents, LLC
4445 Willard Ave.
Suite 600
Chevy Chase, MARYLAND 20815

OC000000073079801

Date Mailed: 05/28/2024

NOTICE OF REEXAMINATION REQUEST FILING DATE

(Third Party Requester)

Requester is hereby notified that the filing date of the request for reexamination is 05/22/2024, the date that the filing requirements of 37 CFR § 1.510 were received.

A decision on the request for reexamination will be mailed within three months from the filing date of the request for reexamination. (See 37 CFR 1.515(a)).

A copy of the Notice is being sent to the person identified by the requester as the patent owner. Further patent owner correspondence will be the latest attorney or agent of record in the patent file. (See 37 CFR 1.33). Any paper filed should include a reference to the present request for reexamination (by Reexamination Control Number).

cc: Patent Owner
23446
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

/rbell/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

AA/SWA Ex. 1015, p.372 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

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.
90/019,519	05/22/2024	7949785	IVI785	2698

23446 7590 05/30/2024
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
05/30/2024	PAPER

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Unified Patents, LLC
4445 Willard Avenue
Suite 600
Chevy Chase, MD 20815

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/019,519* .

PATENT UNDER REEXAMINATION *7949785* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

/PMartin, Paralegal/

PTOL-465 (Rev.07-04)

Ex Parte Reexamination Interview Summary – Pilot Program for Waiver of Patent Owner's Statement	**Control No.** 90/019,519	**Patent Under Reexamination is Requested** 7949785	
	Examiner Dennis Bonshock	**Art Unit** 3992	**AIA (FITF) Status** No

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

All participants (USPTO official and patent owner):

(1) Patricia Martin (3) _____

(2) Peter McAndrews, 38547 (4) _____

Date of Telephonic Interview: 28 May 2024.

A. The USPTO official requested waiver of the patent owner's statement pursuant to the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.*

☐ The patent owner **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.

☑ The patent owner **did not agree** to waive its right to file a patent owner's statement under 35 U.S.C. 304 at this time.

☐ USPTO personnel were unable to reach the patent owner.**

B. The Patent Owner of record telephoned the Office and indicated they would like to participate in the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.*

☐ The Patent owner of record telephoned the Office and **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.

The patent owner is not required to file a written statement of this telephone communication under 37 CFR 1.560(b) or otherwise. However, any disagreement as to this interview summary must be brought to the immediate attention of the USPTO, and no later than one month from the mailing date of this interview summary. Extensions of time are governed by 37 CFR 1.550(c).

*For more information regarding this pilot program, see *Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings, 75 Fed. Reg.* 47269 (August 5, 2010), available on the USPTO Web site at http://www.uspto.gov/patents/law/notices/2010.jsp.

**The patent owner may contact the USPTO personnel at (571) 272-7705 or at the telephone number provided below if the patent owner decides to waive the right to file a patent owner's statement under 35 U.S.C. 304.

/Patricia Martin/
Paralegal Specialist, OCRU (571) 272-5004
Signature and telephone number of the USPTO official, who contacted, was contacted by, or attempted to contact the patent owner.

cc: Requester (if third party requester)

AA/SWA Ex. 1015, p.375 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Litigation Search Report CRU 3999
Reexam No. 90/019,519

To: Dennis Bonshock	**From: Patricia Martin, Paralegal**
Location: CRU	**Location: OCRU**
Art Unit: 3992	**Phone: (571) 272-5004**
Date: June 3, 2024	

Search Notes

U.S. Patent No. 7,949,785

Litigation: Found

1. Performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.
2. Performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.
3. Performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.
4. Performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.
5. Performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

Paper No. Date: 06/03/2024

Citing References (93)

Treatment	Title	Date	Type	Depth	Headnote(s)
Discussed by	**1.** Liberty Mutual Defendants' 12(B)(3) Motion To Dismiss For Improper Venue INTELLECTUAL VENTURES I LLC and Intellectual Ventures II LLC, Plaintiffs, v. LIBERTY MUTUAL HOLDING COMPANY INC., Liberty Mutual Insurance Company, Li... 2024 WL 2262891, *1+ , E.D.Tex. (Trial Motion, Memorandum and Affidavit)	Jan. 25, 2024	Motion		—
Cited by	**2.** Defendant Symantec Corporation's Supplemental Brief Regarding Venue CUPP CYBERSECURITY LLC et al, v. SYMANTEC CORPORATION, Defendant. 2019 WL 4645717, *1 , N.D.Cal. (Trial Motion, Memorandum and Affidavit)	Jan. 04, 2019	Motion		—
Cited by	**3.** Defendant Symantec Corporation's Supplemental Brief Regarding Venue CUPP CYBERSECURITY, LLC and Cupp Computing AS, Plaintiffs, v. SYMANTEC CORPORATION, Defendant. 2019 WL 6445799, *1 , N.D.Tex. (Trial Motion, Memorandum and Affidavit)	Jan. 04, 2019	Motion		—
—	**4.** FACILITATING THE SENDING OF MAIL FROM A RESTRICTED COMMUNICATIONS NETWORK Out Of Plan US PAT 8583739 , U.S. PTO Utility The sending of mail from a restricted communications network is facilitated. A communications unit external to the restricted communications network periodically pulls the mail...	Nov. 12, 2013	Patents	—	—
—	**5.** METHOD TO TUNNEL UDP-BASED DEVICE DISCOVERY Out Of Plan US PAT 8571038 , U.S. PTO Utility A method, apparatus, and system are described for a central station to allocate virtual IP addresses. A device service manager server (DSM) has a network access module configured...	Oct. 29, 2013	Patents	—	—
—	**6.** SELECTIVELY PROTECTING AGAINST CHOSEN PLAINTEXT ATTACKS IN UNTRUSTED STORAGE ENVIRONMENTS THAT SUPPORT DATA DEDUPLICATION Out Of Plan US PAT 8479304 , U.S. PTO Utility Various methods and systems for selectively protecting against chosen plaintext attacks when encrypting data for storage on an untrusted storage system are disclosed. One method...	July 02, 2013	Patents	—	—
—	**7.** VIRTUAL COMMUNITY NETWORK IMPLEMENTING SYSTEM FOR E.G. SERVER, HAS VIRTUAL COMMUNITY NETWORK MANAGER WITH DEFINITION, WHERE VIRTUAL ADDRESS REALM IS CREATED BY ASSIGNING VIRTUAL IP ADDRESS TO EACH UNIT OF NETWORK Out Of Plan DWPI 2005-063898	Mar. 31, 2003	DWPI	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**8.** RF 065469/0182 Out Of Pat.	Nov. 06, 2023	Assignments	—	—
—	**9.** RF 037490/0592 Out Of Pat.	Jan. 14, 2016	Assignments	—	—
—	**10.** RF 020393/0423 Out Of Pat.	Jan. 21, 2008	Assignments	—	—
—	**11.** RF 014340/0968 Out Of Pat.	Aug. 04, 2003	Assignments	—	—
—	**12.** RF 014196/0265 Out Of Pat.	June 24, 2003	Assignments	—	—
—	**13.** Assurant, Inc. v. Intellectual Ventures I LLC ET AL	Mar. 15, 2024	Docket Summaries	—	—
—	**14.** Intellectual Ventures I LLC ET AL v. JP Morgan Chase & Co.	Nov. 15, 2023	Docket Summaries	—	—
—	**15.** Intellectual Ventures I LLC ET AL v. Comerica Incorporated	Nov. 15, 2023	Docket Summaries	—	—
—	**16.** Intellectual Ventures I LLC ET AL v. Liberty Mutual Holding Company Inc. ET AL	Nov. 15, 2023	Docket Summaries	—	—
—	**17.** ANONYMIZING SERVER-SIDE ADDRESSES Out Of Pat. US PAT 11979366 , U.S. PTO Utility Techniques for using Network Address Translation (NAT), Mobile Internet Protocol (MIP), and/or other techniques in conjunction with Domain Name System (DNS) to anonymize...	May 07, 2024	Patents	—	—
—	**18.** REQUEST ROUTING BASED ON CLASS Out Of Pat. US PAT 11909639 , U.S. PTO Utility A system and method for management and processing of resource requests is provided. A content delivery network service provider receives a DNS query from a client computing device....	Feb. 20, 2024	Patents	—	—
—	**19.** COORDINATING INTER-REGION OPERATIONS IN PROVIDER NETWORK ENVIRONMENTS Out Of Pat. US PAT 11902367 , U.S. PTO Utility Methods and apparatus for coordinating inter-region operations in provider networks. An inter-region coordinator (IRC) operates asynchronously to the control planes of regional...	Feb. 13, 2024	Patents	—	—
—	**20.** ROUTING MODE AND POINT-OF-PRESENCE SELECTION SERVICE Out Of Pat. US PAT 11863417 , U.S. PTO Utility Systems and methods for sloppy routing are provided. A client transmits a DNS query corresponding to a requested resource to a content delivery network (CDN) service provider. In...	Jan. 02, 2024	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**21.** SYSTEMS, METHODS, AND MEDIA FOR DEFENDING COMPUTING SYSTEMS FROM ATTACK Out Of Plan US PAT 11831418 , U.S. PTO Utility Mechanisms for defending a computing system from attack are provided. The mechanisms include: maintaining a round counter that tracks a round number for a local host; determining a...	Nov. 28, 2023	Patents	—	—
—	**22.** AUTHORITATIVE DOMAIN NAME SYSTEM (DNS) SERVER RESPONDING TO DNS REQUESTS WITH IP ADDRESSES SELECTED FROM A LARGER POOL OF IP ADDRESSES Out Of Plan US PAT 11818167 , U.S. PTO Utility An authoritative DNS server receives DNS requests for domains. The authoritative DNS server responds to the requests with address records that include IP addresses that are...	Nov. 14, 2023	Patents	—	—
—	**23.** UPDATING ROUTING INFORMATION BASED ON CLIENT LOCATION Out Of Plan US PAT 11811657 , U.S. PTO Utility A system, method, and computer-readable medium for updating request routing information associated with client location information are provided. A content delivery network service...	Nov. 07, 2023	Patents	—	—
—	**24.** PRIVATE NETWORK PEERING IN VIRTUAL NETWORK ENVIRONMENTS Out Of Plan US PAT 11770364 , U.S. PTO Utility Methods and apparatus for private network peering in virtual network environments in which peerings between virtual client private networks on a provider network may be established...	Sep. 26, 2023	Patents	—	—
—	**25.** MULTI-REGION REQUEST-DRIVEN CODE EXECUTION SYSTEM Out Of Plan US PAT 11762703 , U.S. PTO Utility An on-demand code execution environment present in points of presence (POPs) and in regions serviced by the POPs is provided herein. For example, a POP may receive a request to...	Sep. 19, 2023	Patents	—	—
—	**26.** PROCESSING DNS QUERIES TO IDENTIFY PRE-PROCESSING INFORMATION Out Of Plan US PAT 11729294 , U.S. PTO Utility Systems and methods for processing a DNS query to identify and implement pre-processing information by a DNS server component in anticipation of a corresponding content request...	Aug. 15, 2023	Patents	—	—
—	**27.** REVERSE FORWARDING INFORMATION BASE ENFORCEMENT Out Of Plan US PAT 11722405 , U.S. PTO Utility In exemplary embodiments of the present invention, a router determines whether or not to establish a stateful routing session based on the suitability of one or more candidate...	Aug. 08, 2023	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**28.** POINT OF PRESENCE MANAGEMENT IN REQUEST ROUTING Out Of Plan US PAT 11632420 , U.S. PTO Utility A system and method for the management of client computing device DNS queries and subsequent resource requests within a content delivery network service provider domain are...	Apr. 18, 2023	Patents	—	—
—	**29.** OPTIMIZED DEPLOYMENT BASED UPON CUSTOMER LOCALITY Out Of Plan US PAT 11604667 , U.S. PTO Utility The deployment of content and computing resources for implementing a distributed software application can be optimized based upon customer location. The volume and geographic...	Mar. 14, 2023	Patents	—	—
—	**30.** COORDINATING INTER-REGION OPERATIONS IN PROVIDER NETWORK ENVIRONMENTS Out Of Plan US PAT 11582298 , U.S. PTO Utility Methods and apparatus for coordinating inter-region operations in provider networks. An inter-region coordinator (IRC) operates asynchronously to the control planes of regional...	Feb. 14, 2023	Patents	—	—
—	**31.** ROUTING BASED REQUEST CORRELATION Out Of Plan US PAT 11461402 , U.S. PTO Utility Aspects of the disclosure will be described with regard to the processing of DNS queries by a DNS service based on multiple network addresses associated with a single network...	Oct. 04, 2022	Patents	—	—
—	**32.** REQUEST MANAGEMENT FOR HIERARCHICAL CACHE Out Of Plan US PAT 11463550 , U.S. PTO Utility A computer implemented cache management system and method is provided for use with a service provider configured to communicate with one or more client devices and with a content...	Oct. 04, 2022	Patents	—	—
—	**33.** ADAPTIVE TRANSFER RATE FOR RETRIEVING CONTENT FROM A SERVER Out Of Plan US PAT 11457088 , U.S. PTO Utility An edge system receives requests from user devices to retrieves files from an origin server. Instead of retrieving the files as fast as possible, the edge system throttles the...	Sep. 27, 2022	Patents	—	—
—	**34.** REQUEST ROUTING BASED ON CLASS Out Of Plan US PAT 11451472 , U.S. PTO Utility A system and method for management and processing of resource requests is provided. A content delivery network service provider receives a DNS query from a client computing device....	Sep. 20, 2022	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**35.** ROUTING MODE AND POINT-OF-PRESENCE SELECTION SERVICE Out Of Fam. US PAT 11381487 , U.S. PTO Utility Systems and methods for sloppy routing are provided. A client transmits a DNS query corresponding to a requested resource to a content delivery network (CDN) service provider. In...	July 05, 2022	Patents	—	—
—	**36.** RESOLUTION OF DOMAIN NAME REQUESTS IN HETEROGENEOUS NETWORK ENVIRONMENTS Out Of Fam. US PAT 11362986 , U.S. PTO Utility Systems and methods are for domain name system (DNS) resolutions in heterogeneous network environments including a virtual private cloud (VPC). An administrator of a virtual...	June 14, 2022	Patents	—	—
—	**37.** POINT OF PRESENCE MANAGEMENT IN REQUEST ROUTING Out Of Fam. US PAT 11336712 , U.S. PTO Utility A system and method for the management of client computing device DNS queries and subsequent resource requests within a content delivery network service provider domain are...	May 17, 2022	Patents	—	—
—	**38.** NETWORK ADDRESSES WITH ENCODED DNS-LEVEL INFORMATION Out Of Fam. US PAT 11330008 , U.S. PTO Utility Systems and methods are described to enable a DNS service to encode information into a network address to be advertised by the DNS service. Information encoded by a DNS service may...	May 10, 2022	Patents	—	—
—	**39.** SYSTEMS, METHODS, AND MEDIA FOR DEFENDING COMPUTING SYSTEMS FROM ATTACK Out Of Fam. US PAT 11310249 , U.S. PTO Utility Mechanisms for defending a computing system from attack are presented. The mechanisms include: maintaining a round counter that tracks a round number for a local host; determining...	Apr. 19, 2022	Patents	—	—
—	**40.** PROCESSING DNS QUERIES TO IDENTIFY PRE-PROCESSING INFORMATION Out Of Fam. US PAT 11303717 , U.S. PTO Utility Systems and methods for processing a DNS query to identify and implement pre-processing information by a DNS server component in anticipation of a corresponding content request...	Apr. 12, 2022	Patents	—	—
—	**41.** POINT OF PRESENCE BASED DATA UPLOADING Out Of Fam. US PAT 11297140 , U.S. PTO Utility A system, method and computer-readable medium for data uploading based on points of presence (POPs) are provided. In response to a client's request for data uploading, the system...	Apr. 05, 2022	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**42.** HYBRID CONTENT REQUEST ROUTING SYSTEM Out Of Plan US PAT 11290418 , U.S. PTO Utility A hybrid content request routing system is described herein. The hybrid content request routing system may use aspects of the anycast routing technique and aspects of the domain...	Mar. 29, 2022	Patents	—	—
—	**43.** UPDATING ROUTING INFORMATION BASED ON CLIENT LOCATION Out Of Plan US PAT 11283715 , U.S. PTO Utility A system, method, and computer-readable medium for updating request routing information associated with client location information are provided. A content delivery network service...	Mar. 22, 2022	Patents	—	—
—	**44.** LOCALITY BASED CONTENT DISTRIBUTION Out Of Plan US PAT 11245770 , U.S. PTO Utility A system and method for content distribution are provided. A content provider generates a network topology having one or more subnetworks made up of content sources. The content...	Feb. 08, 2022	Patents	—	—
—	**45.** AUTHORIZING COMMUNICATIONS BETWEEN COMPUTING NODES Out Of Plan US PAT 11240092 , U.S. PTO Utility Techniques are described for managing communications between multiple computing nodes, such as computing nodes that are separated by one or more physical networks. In some...	Feb. 01, 2022	Patents	—	—
—	**46.** IDENTIFYING A DENIAL-OF-SERVICE ATTACK IN A CLOUD-BASED PROXY SERVICE Out Of Plan US PAT 11159563 , U.S. PTO Utility A cloud-based proxy service identifies a denial-of-service (DoS) attack including determining that there is a potential DoS attack being directed to an IP address of the...	Oct. 26, 2021	Patents	—	—
—	**47.** COORDINATING INTER-REGION OPERATIONS IN PROVIDER NETWORK ENVIRONMENTS Out Of Plan US PAT 11102291 , U.S. PTO Utility Methods and apparatus for coordinating inter-region operations in provider networks. An inter-region coordinator (IRC) operates asynchronously to the control planes of regional...	Aug. 24, 2021	Patents	—	—
—	**48.** PRIVATE NETWORK LAYERING IN PROVIDER NETWORK ENVIRONMENTS Out Of Plan US PAT 11089021 , U.S. PTO Utility Methods and apparatus that allow clients to establish sub private networks as resources within private networks on a provider network. A sub private network may be owned and...	Aug. 10, 2021	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**49.** REVERSE FORWARDING INFORMATION BASE ENFORCEMENT Out Of Plan US PAT 11075836 , U.S. PTO Utility In exemplary embodiments of the present invention, a router determines whether or not to establish a stateful routing session based on the suitability of one or more candidate...	July 27, 2021	Patents	—	—
—	**50.** MULTIPLEXING TRAFFIC FROM MULTIPLE NETWORK NAMESPACES TO A SINGLE LISTENER IN A STREAM-BASED SERVER APPLICATION Out Of Plan US PAT 10897488 , U.S. PTO Utility Techniques of operating a server computer running an application for clients operating in multiple network namespaces involve multiplexing communications streams from clients...	Jan. 19, 2021	Patents	—	—
—	**51.** PRIVATE NETWORK PEERING IN VIRTUAL NETWORK ENVIRONMENTS Out Of Plan US PAT 10893024 , U.S. PTO Utility Methods and apparatus for private network peering in virtual network environments in which peerings between virtual client private networks on a provider network may be established...	Jan. 12, 2021	Patents	—	—
—	**52.** DNS OR NETWORK METADATA POLICY FOR NETWORK CONTROL Out Of Plan US PAT 10868833 , U.S. PTO Utility Techniques for configuring a network based on a Domain Name System (DNS) or network metadata policy for network control are disclosed. In some embodiments, a system, process,...	Dec. 15, 2020	Patents	—	—
—	**53.** FLOW MODIFICATION INCLUDING SHARED CONTEXT Out Of Plan US PAT 10841206 , U.S. PTO Utility Routing packets by a router involves establishing a first flow configured for forwarding the packets from a first ingress interface to a first egress interface of the router;...	Nov. 17, 2020	Patents	—	—
—	**54.** NAT TRAVERSAL FOR MEDIA CONFERENCING Out Of Plan US PAT 10630730 , U.S. PTO Utility Methods for establishing a direct peer-to-peer ("P2P") connection between two computers are disclosed. In particular, the methods are designed to work in cases where one or both...	Apr. 21, 2020	Patents	—	—
—	**55.** AUTHORIZING COMMUNICATIONS BETWEEN COMPUTING NODES Out Of Plan US PAT 10601708 , U.S. PTO Utility Techniques are described for managing communications between multiple computing nodes, such as computing nodes that are separated by one or more physical networks. In some...	Mar. 24, 2020	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**56.** RULE ENFORCEMENT BASED ON NETWORK ADDRESS REQUESTS Out Of Plan US PAT 10560480 , U.S. PTO Utility A first device may include one or more processors. The first device may receive a network address request to obtain a network address that is associated with an application. The...	Feb. 11, 2020	Patents	—	—
—	**57.** TECHNIQUES FOR DOMAIN CAPTURE Out Of Plan US PAT 10523651 , U.S. PTO Utility Techniques for domain capture. In one embodiment, for example, a method comprises detecting an attempt by a personal user account to use the online service where the account is...	Dec. 31, 2019	Patents	—	—
—	**58.** MITIGATING A DENIAL-OF-SERVICE ATTACK IN A CLOUD-BASED PROXY SERVICE Out Of Plan US PAT 10511624 , U.S. PTO Utility A proxy server in a cloud-based proxy service receives a message that indicates that a domain, whose traffic passes through the proxy server, may be under a denial-of-service (DoS)...	Dec. 17, 2019	Patents	—	—
—	**59.** COORDINATING INTER-REGION OPERATIONS IN PROVIDER NETWORK ENVIRONMENTS Out Of Plan US PAT 10498810 , U.S. PTO Utility Methods and apparatus for coordinating inter-region operations in provider networks. An inter-region coordinator (IRC) operates asynchronously to the control planes of regional...	Dec. 03, 2019	Patents	—	—
—	**60.** AUTOMATIC CREATION AND MANAGEMENT OF A COMMUNITY OF THINGS FOR INTERNET OF THINGS (IOT) APPLICATIONS Out Of Plan US PAT 10476743 , U.S. PTO Utility Presented herein are techniques for automatically creating communities of network-connected devices, i.e., Internet of Thing (IoT) devices. One or more of a plurality of...	Nov. 12, 2019	Patents	—	—
—	**61.** TECHNIQUES FOR INVITE ENFORCEMENT Out Of Plan US PAT 10348717 , U.S. PTO Utility Techniques for invite enforcement. In one embodiment, for example, a method comprises: receiving an acceptance of an invitation to join a team of one or more team user accounts...	July 09, 2019	Patents	—	—
—	**62.** SYSTEM AND METHOD FOR TRAVERSING A NAT DEVICE WITH IPSEC AH AUTHENTICATION Out Of Plan US PAT 10333919 , U.S. PTO Utility A method for routing IP packets with IPSec AH authentication is disclosed. The method includes locating overlay edge routers between private domains and their associated NAT...	June 25, 2019	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**63.** TECHNIQUES FOR DOMAIN CAPTURE Out Of Plan US PAT 10326751 , U.S. PTO Utility Techniques for domain capture. In one embodiment, for example, a method comprises detecting an attempt to create a personal user account with an online service that uses an...	June 18, 2019	Patents	—	—
—	**64.** MAPPING SCHEME EMPLOYED IN AN INFORMATION CENTRIC NETWORK TO MANAGE DOMAIN-BASED SECURITY AND MOBILITY Out Of Plan US PAT 10271253 , U.S. PTO Utility A networking system comprising a virtual group controller in an information centric network configured to enable mobility and security for a plurality of users groups of the...	Apr. 23, 2019	Patents	—	—
—	**65.** DETECTING SOURCE NETWORK ADDRESS TRANSLATION IN A COMMUNICATION SYSTEM Out Of Plan US PAT 10257061 , U.S. PTO Utility Two nodes in a communication system exchange link monitoring protocol messages including special metadata that allows each node to determine the status of source NAT on...	Apr. 09, 2019	Patents	—	—
—	**66.** AUTHORIZING COMMUNICATIONS BETWEEN COMPUTING NODES Out Of Plan US PAT 10218613 , U.S. PTO Utility Techniques are described for managing communications between multiple computing nodes, such as computing nodes that are separated by one or more physical networks. In some...	Feb. 26, 2019	Patents	—	—
—	**67.** PRIVATE NETWORK LAYERING IN PROVIDER NETWORK ENVIRONMENTS Out Of Plan US PAT 10212161 , U.S. PTO Utility Methods and apparatus that allow clients to establish sub private networks as resources within private networks on a provider network. A sub private network may be owned and...	Feb. 19, 2019	Patents	—	—
—	**68.** LINK STATUS MONITORING BASED ON PACKET LOSS DETECTION Out Of Plan US PAT 10200264 , U.S. PTO Utility In exemplary embodiments of the present invention, special metadata is added to link monitoring protocol messages exchanged by pairs of adjacent nodes to allow such nodes to detect...	Feb. 05, 2019	Patents	—	—
—	**69.** PRIVATE NETWORK PEERING IN VIRTUAL NETWORK ENVIRONMENTS Out Of Plan US PAT 10193866 , U.S. PTO Utility Methods and apparatus for private network peering in virtual network environments in which peerings between virtual client private networks on a provider network may be established...	Jan. 29, 2019	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**70.** SESSION CONTINUITY IN THE PRESENCE OF NETWORK ADDRESS TRANSLATION Ont. Of Plan US PAT 10091099 , U.S. PTO Utility Embodiments of the present invention provide for continuity of "stateful" routing sessions in the presence of source network address translation (NAT). Specifically, a stateful...	Oct. 02, 2018	Patents	—	—
—	**71.** TECHNIQUES FOR INVITE ENFORCEMENT AND DOMAIN CAPTURE Ont. Of Plan US PAT 10079817 , U.S. PTO Utility Techniques for invite enforcement and domain capture. In one embodiment, for example, a method performed in an online service computing environment comprises the operations of:...	Sep. 18, 2018	Patents	—	—
—	**72.** SYSTEM AND METHOD FOR TRAVERSING A NAT DEVICE WITH IPSEC AH AUTHENTICATION Ont. Of Plan US PAT 9942216 , U.S. PTO Utility A method for routing IP packets with IPSec AH authentication is disclosed. The method includes locating overlay edge routers between private domains and their associated NAT...	Apr. 10, 2018	Patents	—	—
—	**73.** METHOD AND SYSTEM FOR ACCESSING NETWORK SERVICE Ont. Of Plan US PAT 9832139 , U.S. PTO Utility According to an example, a web server receives an access request from one operator network of different operator networks, process the access request, and obtain processing data....	Nov. 28, 2017	Patents	—	—
—	**74.** SEPARATING NETWORK TRAFFIC AMONG VIRTUAL SERVERS Ont. Of Plan US PAT 9806984 , U.S. PTO Utility Techniques for routing network traffic in a storage processor involve providing per-IP routing tables for each IP address of a virtual server and a per-server routing table. These...	Oct. 31, 2017	Patents	—	—
—	**75.** PRIVATE NETWORK PEERING IN VIRTUAL NETWORK ENVIRONMENTS Ont. Of Plan US PAT 9807057 , U.S. PTO Utility Methods and apparatus for private network peering in virtual network environments in which peerings between virtual client private networks on a provider network may be established...	Oct. 31, 2017	Patents	—	—
—	**76.** DNS OR NETWORK METADATA POLICY FOR NETWORK CONTROL Ont. Of Plan US PAT 9736185 , U.S. PTO Utility Techniques for configuring a network based on a Domain Name System (DNS) or network metadata policy for network control are disclosed. In some embodiments, a system, process,...	Aug. 15, 2017	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**77.** AUTHORIZING COMMUNICATIONS BETWEEN COMPUTING NODES Out Of Plan US PAT 9705792 , U.S. PTO Utility Techniques are described for managing communications between multiple computing nodes, such as computing nodes that are separated by one or more physical networks. In some...	July 11, 2017	Patents	—	—
—	**78.** SYSTEM AND METHOD FOR TRAVERSING A NAT DEVICE WITH IPSEC AH AUTHENTICATION Out Of Plan US PAT 9641551 , U.S. PTO Utility A method for routing IP packets with IPSec AH authentication is disclosed. The method includes locating overlay edge routers between private domains and their associated NAT...	May 02, 2017	Patents	—	—
—	**79.** AUTHORIZING COMMUNICATIONS BETWEEN COMPUTING NODES Out Of Plan US PAT 9577926 , U.S. PTO Utility Techniques are described for managing communications between multiple computing nodes, such as computing nodes that are separated by one or more physical networks. In some...	Feb. 21, 2017	Patents	—	—
—	**80.** PEER-TO-PEER MOBILITY MANAGEMENT IN HETEROGENEOUS IPV4 NETWORKS Out Of Plan US PAT 9307393 , U.S. PTO Utility Peer-to-peer mobility management in heterogeneous IP networks provides a peer-to-peer mobility module operable to intercept a data packet received at a communication protocol layer...	Apr. 05, 2016	Patents	—	—
—	**81.** CONTROL PLANE TO MANAGE DOMAIN-BASED SECURITY AND MOBILITY IN AN INFORMATION CENTRIC NETWORK Out Of Plan US PAT 9253215 , U.S. PTO Utility A networking system comprising a virtual group controller in an information centric network configured to enable mobility and security for a plurality of users groups of the...	Feb. 02, 2016	Patents	—	—
—	**82.** METHOD AND APPARATUS FOR ENABLING DNS REDIRECTION IN MOBILE TELECOMMUNICATION SYSTEMS Out Of Plan US PAT 9220051 , U.S. PTO Utility System and method for providing DNS redirection in mobile telecommunication network. The system includes a functionality that is capable of intercepting a DNS reply from a content...	Dec. 22, 2015	Patents	—	—
—	**83.** NETWORK PROTOCOL ANALYZER APPARATUS AND METHOD Out Of Plan US PAT 9100324 , U.S. PTO Utility In one embodiment, a method for electronically analyzing packets using a packet analyzing apparatus includes receiving one or more data packets via a first interface port, wherein...	Aug. 04, 2015	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**84.** FACILITATING THE SENDING OF MAIL FROM A RESTRICTED COMMUNICATIONS NETWORK Out Of Plan US PAT 9065790 , U.S. PTO Utility The sending of mail from a restricted communications network is facilitated. A communications unit external to the restricted communications network periodically pulls the mail...	June 23, 2015	Patents	—	—
—	**85.** METHOD AND SYSTEM FOR FORWARDING DATA BETWEEN NETWORK DEVICES Out Of Plan US PAT 9037724 , U.S. PTO Utility A method and system for forwarding data between network devices is provided. A routing device receives, identifies and forwards data to a network device coupled to a private...	May 19, 2015	Patents	—	—
—	**86.** METHOD AND SYSTEM FOR AGGREGATING COMMUNICATIONS Out Of Plan US PAT 8924486 , U.S. PTO Utility The present invention provides for method, system, and apparatus for facilitating communication between a first set of networked devices, such as client devices, and a second...	Dec. 30, 2014	Patents	—	—
—	**87.** METHOD AND APPARATUS FOR A CONTROL PLANE TO MANAGE DOMAIN-BASED SECURITY AND MOBILITY IN AN INFORMATION CENTRIC NETWORK Out Of Plan US PAT 8881236 , U.S. PTO Utility A networking system comprising a virtual group controller in an information centric network configured to enable mobility and security for a plurality of users groups of the...	Nov. 04, 2014	Patents	—	—
—	**88.** METHOD AND APPARATUS FOR NETWORK PORT AND NETWORK ADDRESS TRANSLATION Out Of Plan US PAT 8812730 , U.S. PTO Utility The present invention provides a method and apparatus for network port and network address translation. Several problems with limited addressability may occur when transmitting...	Aug. 19, 2014	Patents	—	—
—	**89.** SYSTEMS AND METHODS FOR CREATION OF REVERSE VIRTUAL INTERNET PROTOCOL ADDRESSES Out Of Plan US PAT 8793353 , U.S. PTO Utility A method, apparatus, and system are described for a central station to allocate virtual IP addresses. A device service manager server (DSM) has a network access module conFigured...	July 29, 2014	Patents	—	—
—	**90.** VPN SECURE SESSIONS WITH DYNAMIC IP ADDRESSES Out Of Plan US PAT 8356346 , U.S. PTO Utility To help maintain secure and convenient connectivity for users when IP addresses change, devices connected between sites by using multiple virtual private network security...	Jan. 15, 2013	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**91.** PROTECTING AGAINST CHOSEN PLAINTEXT ATTACKS IN UNTRUSTED STORAGE ENVIRONMENTS THAT SUPPORT DATA DEDUPLICATION Out Of Plan US PAT 8281143 , U.S. PTO Utility Various methods and systems for protecting against chosen plaintext attacks when encrypting data for storage on an untrusted storage system are disclosed. One method involves...	Oct. 02, 2012	Patents	—	—
—	**92.** SECURE ENCRYPTION ALGORITHM FOR DATA DEDUPLICATION ON UNTRUSTED STORAGE Out Of Plan US PAT 8199911 , U.S. PTO Utility Various methods and systems for performing data deduplication when encrypting data for storage on an untrusted storage system are disclosed. One method involves generating an...	June 12, 2012	Patents	—	—
—	**93.** SYSTEM AND METHOD FOR ACCESSING A WEB SERVER ON A DEVICE WITH A DYNAMIC IP-ADDRESS RESIDING BEHIND A FIREWALL Out Of Plan US PAT 8190773 , U.S. PTO Utility A system and method for providing access to a web server on an electronic device positioned within a firewall. A gateway device including a gateway server is provided outside of...	May 29, 2012	Patents	—	—

WESTLAW © 2024 Thomson Reuters. No claim to original U.S. Government Works.

User Name: Patricia Martin
Date and Time: Monday, June 3, 2024 4:01:00PM EDT
Job Number: 225730389

Results List (includes up to 250)

1. Results list for:7949785 or 7,949,785
   Client/Matter: -None-
   Terms: 7949785 or 7,949,785
   Search Type: Terms and Connectors
   Narrowed by:

Content Type	Narrowed by
Dockets	Case Status: Open,Unknown,Closed; Case Type: Civil

LexisNexis | About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2024 LexisNexis

LexisNexis

Results for: **7949785 or 7,949,785**

Dockets

1. Assurant, Inc. V. Intellectual Ventures I Llc Et Al

... "IV"). Assurant seeks a declaration that it does not infringe several **patents** owned by IV, including U.S. **Patent** Nos. 10,567,391, 8,332,844, 7,314,167, **7,949,785**, and 7,712,080 (the "DJ **Patents**"). The defendants are related entities that acquire and license **patents**. IV accused Assurant of infringing the DJ **Patents** based on Assurant's use of certain software platforms. IV demanded that ...
... sale, or import any products or systems that infringe the DJ **Patents** . Assurant seeks declaratory judgment of non-infringement to confirm its right ...
... jurisdiction. (mrr) (Entered: 03/18/2024) 3 2024-03-15 Report to the Commissioner of **Patents** and Trademarks for **Patent**/Trademark Number(s) 10,567,391; 8,332,844; 7,314,167; **7,949,785**; 7,712,080. (mrr) (Entered: 03/18/2024) 7588524303 2024-06-02 Report to the Commissioner of **Patents** and Trademarks for **Patent**/Trademark Number(s) 10,567,391; 8,332,844; 7,314,167; **7,949,785**; 7,712,080. (mrr) (Entered: 03/18/2024)...
... Ventures I Llc Et Al 2024-03-15 0 Open CV Civil 830 **Patent** 15 Wilmington 2024-03-18T00:00:00 2024-06-02T00:00:00 2024-03-15 0 **PATENT** Plaintiff 0 None Federal Question Declaratory Judgment 28:2201 0...
... 7,712,080 Systems and methods for parallel distributed programming 2010-05-04 717 119 **7,949,785** Secure virtual community network system 2011-05-24 709 245 9,092,546 Content management ...

Court: United States District Court, Delaware | **Date Filed:** Mar 15, 2024 | **Docket Number:** 1:24cv344 | **Nature of Suit:** Patent | **Cause:** Declaratory Judgment | **Status:** Open

2. Intellectual Ventures I Llc Et Al V. Comerica Incorporated Pursuant To Court Order, Docket In The Lead Case As Directed

... '785 Chart)(Gardner, Allen) (Entered: 11/15/2023) 7588586135 This is a **patent** infringement lawsuit filed by Intellectual Ventures I LLC and Intellectual Ventures ...
... Texas. Intellectual Ventures alleges that Comerica is infringing four of its **patents** related to financial services technologies, including U.S. **Patent** Nos. 8,332,844, 8,407,722, 7,712,080, and **7,949,785**. Specifically, Intellectual Ventures claims Comerica's services that utilize systems like Kubernetes, Docker, Kafka, and Spark infringe the asserted **patents**. Intellectual Ventures seeks damages and an injunction against Comerica for the alleged **patent** infringement. 2024-06-02 COMPLAINT For **Patent** Infringement against Comerica Incorporated (Filing fee $ 402 receipt number ...
... COMPLAINT For **Patent** Infringement against Comerica Incorporated (Filing fee $ 402 receipt number ...
... '785 Chart)(Gardner, Allen) (Entered: 11/15/2023) 2 2023-11-15 Notice of Filing of **Patent**/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. **Patent** and Trademark Office. (Gardner, Allen) (Entered: 11/15/2023) 7588586136 2024-06-02 Notice of Filing of **Patent**/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. **Patent** and Trademark Office. (Gardner, Allen) (Entered: 11/15/2023)...
Patent Infringement 15:1126 0 2024-02-21T00:00:00 0 None 1 2023-11-15 COMPLAINT For **Patent** Infringement against Comerica Incorporated (Filing fee $ 402 receipt number ...

Court: United States District Court, Texas Eastern | **Date Filed:** Nov 15, 2023 | **Docket Number:** 2:23cv524 | **Nature of Suit:** Patent | **Cause:** Patent Infringement | **Status:** Open

AA/SWA Ex. 1015, p.391 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

3. Intellectual Ventures I Llc Et Al V. Jp Morgan Chase Bank, National Association

... '785 Chart)(Gardner, Allen) (Entered: 11/15/2023) 7588030875 This is a **patent** infringement lawsuit filed by Intellectual Ventures I LLC and Intellectual Ventures ...
... Texas. Intellectual Ventures claims that Chase is infringing six of its **patents** related to financial systems and services, including **patents** on asynchronous messaging, virtual data warehousing, parallel distributed programming, secure identification/verification/authorization, ...
... Chase's use of Docker, Kafka, and Spark systems infringes the asserted **patents** . Intellectual Ventures seeks damages adequate to compensate for Chase's alleged ...
... as well as an injunction against further infringement. 2024-06-02 COMPLAINT For **Patent** Infringement against JP Morgan Chase & Co. (Filing fee $ ...
... COMPLAINT For **Patent** Infringement against JP Morgan Chase & Co. (Filing fee $ ...
... '785 Chart)(Gardner, Allen) (Entered: 11/15/2023) 2 2023-11-15 Notice of Filing of **Patent**/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. **Patent** and Trademark Office. (Attachments: # 1 Additional Attachment(s))(Gardner, Allen) (Entered: 11/15/2023) ...
Patent Infringement 15:1126 0 2024-05-17T00:00:00 0 None 1 2023-11-15 COMPLAINT For **Patent** Infringement against JP Morgan Chase & Co. (Filing fee $ ...

Court: United States District Court, Texas Eastern | **Date Filed:** Nov 15, 2023 | **Docket Number:** 2:23cv523 | **Nature of Suit:** Patent | **Cause:** Patent Infringement | **Status:** Open

4. Intellectual Ventures I Llc Et Al V. Liberty Mutual Holding Company Inc. Et Al Pursuant To Court Order, Docket In The Lead Case As Directed

... '785 Chart)(Gardner, Allen) (Entered: 11/15/2023) 7588617441 This is a **patent** infringement lawsuit filed by Intellectual Ventures I LLC and Intellectual Ventures ...
... Ventures alleges that Liberty Mutual is infringing on four of its **patents** related to distributed application management and online backup systems. The defendants ...
... including systems like Kubernetes, Docker, Kafka and Spark, infringe on its **patents**.Intellectual Ventures is seeking damages from Liberty Mutual for the alleged **patent** infringement. The lawsuit claims Liberty Mutual has infringed the **patents** by using, servicing, testing, distributing and/or offering the accused systems and ...
... against Liberty Mutual to prevent continued infringing acts. 2024-06-02 COMPLAINT For **Patent** Infringement against All Defendants (Filing fee $ 402 receipt number ...
... COMPLAINT For **Patent** Infringement against All Defendants (Filing fee $ 402 receipt number ...
... '785 Chart)(Gardner, Allen) (Entered: 11/15/2023) 2 2023-11-15 Notice of Filing of **Patent**/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. **Patent** and Trademark Office. (Gardner, Allen) (Entered: 11/15/2023) 7588617442 2024-06-02 Notice of Filing of **Patent**/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. **Patent** and Trademark Office. (Gardner, Allen) (Entered: 11/15/2023)...
Patent Infringement 15:1126 0 2024-03-26T00:00:00 0 None 1 2023-11-15 COMPLAINT For **Patent** Infringement against All Defendants (Filing fee $ 402 receipt number ...

Court: United States District Court, Texas Eastern | **Date Filed:** Nov 15, 2023 | **Docket Number:** 2:23cv525 | **Nature of Suit:** Patent | **Cause:** Patent Infringement | **Status:** Open

AA/SWA Ex. 1015, p.392 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

User Name: Patricia Martin
Date and Time: Monday, June 3, 2024 4:02:00PM EDT
Job Number: 225730528

Document (1)

1. 1:24cv344, Assurant, Inc. V. Intellectual Ventures I Llc Et Al
   Client/Matter: -None-
   Search Terms: 7949785 or 7,949,785
   Search Type: Terms and Connectors
   Narrowed by:

Content Type	Narrowed by
Dockets	Case Status: Open,Unknown,Closed; Case Type: Civil

LexisNexis | About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2024 LexisNexis

1:24cv344, Assurant, Inc. V. Intellectual Ventures I Llc Et Al

US District Court Docket

United States District Court, Delaware

(Wilmington)

This case was retrieved on 06/02/2024

Header

Case Number: 1:24cv344
Date Filed: 03/15/2024
Assigned To: Judge Gregory B. Williams
Nature of Suit: ***Patent*** (830)
Cause: Declaratory Judgment
Lead Docket: None
Other Docket: None
Jurisdiction: Federal Question

Class Code: Open
Statute: 28:2201
Jury Demand: Plaintiff
Demand Amount: $0
NOS Description: ***Patent***

Participants

Litigants

Assurant, Inc.
Plaintiff

Attorneys

Steven J. Fineman
LEAD ATTORNEY;ATTORNEY TO BE NOTICED
Richards, Layton & Finger, PA
One Rodney Square Suite 600 920 N. King Street
Wilmington, DE 19801
USA
(302) 658-6541 Email:Fineman@rlf.Com

Carter E. Babaz
PRO HAC VICE;ATTORNEY TO BE NOTICED

,

Email:Carter.Babaz@alston.Com

Keith E. Broyles
PRO HAC VICE;ATTORNEY TO BE NOTICED

,

Email:Keith.Broyles@alston.Com

Kelly E. Farnan
ATTORNEY TO BE NOTICED
Richards, Layton & Finger, PA
One Rodney Square Suite 600 920 N. King Street
Wilmington, DE 19801
USA
(302) 651-7705 Email:Farnan@rlf.Com

Patricia Martin

Litigants

Attorneys

Matthew W. Howell
PRO HAC VICE;ATTORNEY TO BE NOTICED

,

Email:Matthew.Howell@alston.Com

Sara M. Metzler
ATTORNEY TO BE NOTICED
Richards, Layton & Finger, PA
One Rodney Square Suite 600 920 N. King Street
Wilmington, DE 19801
USA
(302) 651-7869 Fax: (302) 498-7869
Email:Metzler@rlf.Com

Thomas Finch
PRO HAC VICE;ATTORNEY TO BE NOTICED

,

Email:Thomas.Finch@alston.Com

Intellectual Ventures I LLC
Defendant

Brian E. Farnan
ATTORNEY TO BE NOTICED
Farnan LLP
919 North Market Street 12th Floor
Wilmington, DE 19801
USA
(302) 777-0300 Fax: (302) 777-0301
Email:Bfarnan@farnanlaw.Com

Intellectual Ventures II LLC
Defendant

Brian E. Farnan
ATTORNEY TO BE NOTICED
Farnan LLP
919 North Market Street 12th Floor
Wilmington, DE 19801
USA
(302) 777-0300 Fax: (302) 777-0301
Email:Bfarnan@farnanlaw.Com

Callahan Cellular L.L.C.
Defendant

Brian E. Farnan
ATTORNEY TO BE NOTICED
Farnan LLP
919 North Market Street 12th Floor
Wilmington, DE 19801
USA
(302) 777-0300 Fax: (302) 777-0301
Email:Bfarnan@farnanlaw.Com

Proceedings

#	Date	Proceeding Text	Source
1	03/15/2024	COMPLAINT filed with Jury Demand against Callahan Cellular L.L.C., Intellectual Ventures I LLC, Intellectual Ventures II LLC (Filing fee $ 405, receipt number ADEDC-4363441.) - filed by Assurant, Inc. (Attachments: # 1 Exhibit 1-5, # 2 Civil Cover Sheet)(mrr) (Entered: 03/18/2024)	

#	Date	Proceeding Text	Source
2	03/15/2024	Notice, Consent and Referral forms re: U.S. Magistrate Judge jurisdiction. (mrr) (Entered: 03/18/2024)	
3	03/15/2024	Report to the Commissioner of ***Patents*** and Trademarks for ***Patent***/Trademark Number(s) 10,567,391; 8,332,844; 7,314,167; ***7,949,785***; 7,712,080. (mrr) (Entered: 03/18/2024)	
	03/15/2024	DEFICIENCY NOTICE issued by the Court to Plaintiff: Pursuant to Fed. R. Civ. P. 7.1 (b)(1), A party must: (1) file the disclosure statement with its first appearance, pleading, petition, motion, response, or other request addressed to the court. Counsel is requested to supplement the docket with an appropriate Rule 7.1 Disclosure Statement. (mrr) (Entered: 03/18/2024)	
4	03/15/2024	Summons Issued as to Callahan Cellular L.L.C. on 3/15/2024; Intellectual Ventures I LLC on 3/15/2024; Intellectual Ventures II LLC on 3/15/2024. (Attachments: # 1 Summons Issued, # 2 Summons Issued)(mrr) (Entered: 03/18/2024)	
5	03/18/2024	Disclosure Statement pursuant to Rule 7.1: No Parents or Affiliates Listed filed by Assurant, Inc.. (Farnan, Kelly) (Entered: 03/18/2024)	
6	03/19/2024	SUMMONS Returned Executed by Assurant, Inc..Intellectual Ventures I LLC served on 3/18/2024, answer due 4/8/2024. (Metzler, Sara) (Entered: 03/19/2024)	
7	03/19/2024	SUMMONS Returned Executed by Assurant, Inc..Intellectual Ventures II LLC served on 3/18/2024, answer due 4/8/2024. (Metzler, Sara) (Entered: 03/19/2024)	
8	03/19/2024	SUMMONS Returned Executed by Assurant, Inc..Callahan Cellular L.L.C. served on 3/18/2024, answer due 4/8/2024. (Metzler, Sara) (Entered: 03/19/2024)	
	03/20/2024	Case Assigned to Judge Gregory B. Williams. Please include the initials of the Judge (GBW) after the case number on all documents filed. (rjb) (Entered: 03/20/2024)	
9	03/20/2024	MOTION for Pro Hac Vice Appearance of Attorney Keith Broyles, Matthew W. Howell, Thomas Finch, and Carter E. Babaz - filed by Assurant, Inc.. (Metzler, Sara) (Entered: 03/20/2024)	
10	03/20/2024	Pro Hac Vice Fee - Credit Card Payment received for Keith Broyles, Matthew W. Howell, Thomas Finch, and Carter E. Babaz. (re 9 MOTION for Pro Hac Vice Appearance of Attorney Keith Broyles, Matthew W. Howell, Thomas Finch, and Carter E. Babaz)(Payment of $ 200, receipt number ADEDC-4366900).(Metzler, Sara) (Entered: 03/20/2024)	
	03/21/2024	SO ORDERED, re 9 MOTION for Pro Hac Vice Appearance of Attorney Keith Broyles, Matthew W. Howell, Thomas Finch, and Carter E. Babaz filed by Assurant, Inc. Signed by Judge Gregory B. Williams on 3/21/24. (ntl) (Entered: 03/21/2024)	
11	03/29/2024	STIPULATION TO EXTEND TIME to Respond to Complaint to May 8, 2024 - filed by Callahan Cellular L.L.C., Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Farnan, Brian) (Entered: 03/29/2024)	
	04/02/2024	SO ORDERED, re 11 STIPULATION TO EXTEND TIME to Respond to Complaint to May 8, 2024 filed by Callahan Cellular L.L.C., Intellectual Ventures II LLC, Intellectual Ventures I LLC. Signed by Judge Gregory B. Williams on 4/2/24. (ntl) (Entered: 04/02/2024)	
	04/02/2024	Pro Hac Vice Attorney Matthew W. Howell for Assurant, Inc. added for electronic noticing. Pursuant to Local Rule 83.5 (d)., Delaware counsel shall be the registered users of CM/ECF and shall be required to file all papers. (oam) (Entered: 04/02/2024)	
	04/02/2024	Pro Hac Vice Attorney Carter E. Babaz for Assurant, Inc. added for electronic noticing. Pursuant to Local Rule 83.5 (d)., Delaware	

#	Date	Proceeding Text	Source
		counsel shall be the registered users of CM/ECF and shall be required to file all papers. (oam) (Entered: 04/02/2024)	
	04/02/2024	Pro Hac Vice Attorney Keith E. Broyles for Assurant, Inc. added for electronic noticing. Pursuant to Local Rule 83.5 (d)., Delaware counsel shall be the registered users of CM/ECF and shall be required to file all papers. (oam) (Entered: 04/02/2024)	
	04/02/2024	Pro Hac Vice Attorney Thomas Finch for Assurant, Inc. added for electronic noticing. Pursuant to Local Rule 83.5 (d)., Delaware counsel shall be the registered users of CM/ECF and shall be required to file all papers. (oam) (Entered: 04/02/2024)	
	04/02/2024	Pro Hac Vice Attorney Matthew W. Howell for Assurant, Inc. added for electronic noticing. Pursuant to Local Rule 83.5 (d)., Delaware counsel shall be the registered users of CM/ECF and shall be required to file all papers. (oam) (Entered: 04/02/2024)	
12	05/07/2024	STIPULATION to Seal by Callahan Cellular L.L.C., Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Farnan, Brian) (Entered: 05/07/2024)	
	05/08/2024	SO ORDERED, re 12 STIPULATION to Seal filed by Callahan Cellular L.L.C., Intellectual Ventures II LLC, Intellectual Ventures I LLC. Signed by Judge Gregory B. Williams on 5/8/2024. (lnb) (Entered: 05/08/2024)	
13	05/08/2024	MOTION to Dismiss for Lack of Jurisdiction Over the Subject Matter - filed by Callahan Cellular L.L.C., Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Text of Proposed Order)(Farnan, Brian) (Entered: 05/08/2024)	
14	05/08/2024	OPENING BRIEF in Support re 13 MOTION to Dismiss for Lack of Jurisdiction Over the Subject Matter filed by Callahan Cellular L.L.C., Intellectual Ventures I LLC, Intellectual Ventures II LLC.Answering Brief/Response due date per Local Rules is 5/22/2024. (Farnan, Brian) (Entered: 05/08/2024)	
15	05/08/2024	[SEALED] DECLARATION re 14 Opening Brief in Support, of Jonathan K. Waldrop by Callahan Cellular L.L.C., Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Exhibit 7)(Farnan, Brian) (Entered: 05/08/2024)	
16	05/15/2024	REDACTED VERSION of 15 Declaration, by Callahan Cellular L.L.C., Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Exhibits 1-7)(Farnan, Brian) (Entered: 05/15/2024)	
17	05/21/2024	STIPULATION TO EXTEND TIME for Plaintiff to file its Answering Brief is extended through and including June 5, 2024 and the deadline for Defendants to file their Reply Brief is extended to through and including June 26, 2024 - filed by Assurant, Inc.. (Farnan, Kelly) (Entered: 05/21/2024)	
	05/22/2024	SO ORDERED, re 17 STIPULATION TO EXTEND TIME for Plaintiff to file its Answering Brief is extended through and including June 5, 2024 and the deadline for Defendants to file their Reply Brief is extended to through and including June 26, 2024 filed by Assurant, Inc. Signed by Judge Gregory B. Williams on 5/22/2024. (lnb) (Entered: 05/22/2024)	

Patents

Number	Title	Issued	Class	Subclass
7,199,715	System and method for tracking ID tags using a data structure of tag reads	04/03/2007	340	572.1
7,712,080	Systems and methods for parallel distributed programming	05/04/2010	717	119

Number	Title	Issued	Class	Subclass
7,949,785	Secure virtual community network system	05/24/2011	709	245
9,092,546	Content management and transformation system for digital content	07/28/2015	1	1
9,686,378	Content management and transformation system for digital content	06/20/2017	1	1
10,567,391	Graduated authentication in an identity management system	02/18/2020	1	1

Copyright © LexisNexis CourtLink, Inc. All Rights Reserved.
*** THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY ***

End of Document

User Name: Patricia Martin
Date and Time: Monday, June 3, 2024 4:02:00PM EDT
Job Number: 225730620

Document (1)

1. 2:23cv624, Intellectual Ventures I Llc Et Al V. Comerica Incorporated, Pursuant To Court Order, Docket In The Lead Case As Directed

Client/Matter: -None-
Search Terms: 7949785 or 7,949,785
Search Type: Terms and Connectors
Narrowed by:

Content Type	Narrowed by
Dockets	Case Status: Open,Unknown,Closed; Case Type: Civil

LexisNexis | About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2024 LexisNexis

2:23cv524, Intellectual Ventures I Llc Et Al V. Comerica Incorporated Pursuant To Court Order, Docket In The Lead Case As Directed

US District Court Docket

United States District Court, Texas Eastern

(Marshall)

This case was retrieved on 06/02/2024

Header

Case Number: 2:23cv524
Date Filed: 11/15/2023
Assigned To: District Judge Rodney Gilstrap
Nature of Suit: ***Patent*** (830)
Cause: ***Patent*** Infringement
Lead Docket: 2:23cv00523
Other Docket: None
Jurisdiction: Federal Question

Class Code: Open
Statute: 15:1126
Jury Demand: Plaintiff
Demand Amount: $0
NOS Description: ***Patent***

Participants

Litigants	Attorneys
Intellectual Ventures I LLC **Plaintiff**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Intellectual Ventures II LLC **Plaintiff**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner
	Patricia Martin

2:23cv524, Intellectual Ventures I Llc Et Al V. Comerica Incorporated Pursuant To Court Order, Docket In The Lead Case As Directed

Litigants

Attorneys

ATTORNEY TO BE NOTICED
Allen Gardner Law, PLLC
609 South Fannin
Tyler, TX 75701
USA
903-944-7537 Fax: 903-944-7856
Email:Allen@allengardnerlaw.Com

Comerica Incorporated
Defendant

Joshua David Curry
ATTORNEY TO BE NOTICED
Lewis Brisbois Bisgaard & Smith
600 Peachtree Street, Ne Suite 4700
Atlanta, GA 30308
USA
404-348-8585 Email:Josh.Curry@lewisbrisbois.Com

Proceedings

#	Date	Proceeding Text	Source
1	11/15/2023	COMPLAINT For ***Patent*** Infringement against Comerica Incorporated (Filing fee $ 402 receipt number ATXEDC-9818688.), filed by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Civil Cover Sheet, # 2 Exhibit 1 - US8332844, # 3 Exhibit 2 - US8407722, # 4 Exhibit 3 - US7712080B2, # 5 Exhibit 4 - US7949785, # 6 Exhibit 5 - Notice Letter, # 7 Exhibit 6 - '844 Chart, # 8 Exhibit 7 - '722 Chart, # 9 Exhibit 8 - '080 Chart, # 10 Exhibit 9 - '785 Chart)(Gardner, Allen) (Entered: 11/15/2023)	
2	11/15/2023	Notice of Filing of ***Patent***/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. ***Patent*** and Trademark Office. (Gardner, Allen) (Entered: 11/15/2023)	
3	11/15/2023	Fed. R. Civ. P. 7.1(a)(1) Disclosure Statement filed by Intellectual Ventures I LLC, Intellectual Ventures II LLC (Gardner, Allen) (Entered: 11/15/2023)	
4	11/15/2023	DEMAND for Trial by Jury by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Gardner, Allen) (Entered: 11/15/2023)	
	11/15/2023	District Judge Rodney Gilstrap added. (klc,) (Entered: 11/15/2023)	
5	11/15/2023	SUMMONS Issued as to Comerica Incorporated. (nkl,) (Entered: 11/15/2023)	
6	11/22/2023	SUMMONS Returned Executed by Intellectual Ventures I LLC, Intellectual Ventures II LLC. Comerica Incorporated served on 11/20/2023. (Gardner, Allen) (Entered: 11/22/2023)	
7	12/22/2023	Defendant's Unopposed First Application for Extension of Time to Answer Complaint re Comerica Incorporated.(Curry, Joshua) (Entered: 12/22/2023)	
	12/26/2023	Defendant's Unopposed First Application for Extension of Time to Answer Complaint is granted pursuant to Local Rule CV-12 for Comerica Incorporated to 1/17/2024. (klc,) (Entered: 12/26/2023)	
8	01/16/2024	Defendant's Unopposed Second Application for Extension of Time to Answer Complaint re Comerica Incorporated.(Curry, Joshua) (Entered: 01/16/2024)	
9	01/17/2024	UNOPPOSED MOTION for Extension of Time to File Answer re 1 Complaint,, Unopposed Motion for Second Extension of Time for Defendant to Answer or Otherwise Respond to Complaint by	

#	Date	Proceeding Text	Source
		Comerica Incorporated. (Attachments: # 1 Proposed Order)(Curry, Joshua) (Entered: 01/17/2024)	
10	01/22/2024	ORDER granting 9 UNOPPOSED MOTION for Extension of Time to File Answer re 1 Complaint, Comerica Incorporated answer due 2/16/2024. Signed by District Judge Rodney Gilstrap on 1/19/2024. (nkl,) (Entered: 01/22/2024)	
11	02/13/2024	CONSOLIDATION ORDER - The above-captioned cases are hereby ORDERED to be CONSOLIDATED for allpretrial issues with the LEAD CASE, Case No. 2:23-cv-00523. All parties are any future filings in the LEAD CASE. Individual cases remain active for trial. Signed by District Judge Rodney Gilstrap on 2/13/2024. (ch,) (Entered: 02/13/2024)	
12	02/21/2024	NOTICE of Readiness for Scheduling Conference by Intellectual Ventures I LLC, Intellectual Ventures II LLC (Waldrop, Jonathan) (Entered: 02/21/2024)	

Patents

Number	Title	Issued	Class	Subclass
7,712,080	Systems and methods for parallel distributed programming	05/04/2010	717	119
7,949,785	Secure virtual community network system	05/24/2011	709	245
8,407,722	Asynchronous messaging using a node specialization architecture in the dynamic routing network	03/26/2013	719	316

Copyright © LexisNexis CourtLink, Inc. All Rights Reserved.
*** THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY ***

End of Document

User Name: Patricia Martin
Date and Time: Monday, June 3, 2024 4:03:00PM EDT
Job Number: 225730748

Document (1)

1. 2:23cv623, Intellectual Ventures I Llc Et Al V. Jp Morgan Chase Bank, National Association

Client/Matter: -None-
Search Terms: 7949785 or 7,949,785
Search Type: Terms and Connectors
Narrowed by:

Content Type	Narrowed by
Dockets	Case Status: Open,Unknown,Closed; Case Type: Civil

LexisNexis | About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2024 LexisNexis

2:23cv523, Intellectual Ventures I Llc Et Al V. Jp Morgan Chase Bank, National Association

US District Court Docket

United States District Court, Texas Eastern

(Marshall)

This case was retrieved on 06/02/2024

Header

Case Number: 2:23cv523
Date Filed: 11/15/2023
Assigned To: District Judge Rodney Gilstrap
Nature of Suit: ***Patent*** (830)
Cause: ***Patent*** Infringement
Lead Docket: None
Other Docket: None
Jurisdiction: Federal Question

Class Code: Open
Statute: 15:1126
Jury Demand: Both
Demand Amount: $0
NOS Description: ***Patent***

Participants

Litigants	Attorneys
Intellectual Ventures I LLC **Plaintiff**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Intellectual Ventures II LLC **Plaintiff**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED
Patricia Martin	

Litigants	Attorneys
	Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
JP Morgan Chase & Co. [Terminated: 03/14/2024] **Defendant**	Benjamin Hershkowitz ATTORNEY TO BE NOTICED [Terminated: 03/15/2024] Gibson Dunn & Crutcher, LLP - NYC 200 Park Ave 48th Floor New York, NY 10166-0193 USA 212-351-2410 Fax: 212-351-6210 Email:Bhershkowitz@gibsondunn.Com Katherine Dominguez ATTORNEY TO BE NOTICED [Terminated: 03/15/2024] Gibson Dunn & Crutcher, LLP - NYC 200 Park Ave 48th Floor New York, NY 10166-0193 USA 212-351-2338 Fax: 212-351-4035 Email:Kdominguez@gibsondunn.Com Melissa Richards Smith ATTORNEY TO BE NOTICED [Terminated: 03/15/2024] Gillam & Smith, LLP 303 South Washington Avenue Marshall, TX 75670 USA 903-934-8450 Fax: 903-934-9257 Email:Melissa@gillamsmithlaw.Com Nathan Robert Curtis ATTORNEY TO BE NOTICED [Terminated: 03/15/2024] Gibson, Dunn & Crutcher LLC - Dallas 2001 Ross Avenue Suite 2100 Dallas, TX 75201 USA 214-698-3423 Fax: 214-571-2961 Email:Ncurtis@gibsondunn.Com
JP Morgan Chase Bank, National Association [Terminated: 05/17/2024] **Defendant**	Melissa Richards Smith ATTORNEY TO BE NOTICED [Terminated: 05/17/2024] Gillam & Smith, LLP 303 South Washington Avenue Marshall, TX 75670 USA 903-934-8450 Fax: 903-934-9257 Email:Melissa@gillamsmithlaw.Com
Comerica Incorporated Consolidated from 2:23-cv-524 | **Consol Defendant**	Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402

Litigants	Attorneys
	USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000 Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com
Liberty Mutual Holding Company Inc. Consolidated from 2:23-cv-525 | **Consol Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Jonathan Goins ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith Bank Of America Plaza 600 Peachtree Street Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Fax: 404-467-8845 Email:Jonathan.Goins@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000

Litigants	Attorneys
	Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com Meleah Marie Skillern ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 1 Gojo Plaza Ste #310 Akron, OH 44311 USA 330-272-0000 Fax: 330-272-0019 Email:Meleah.Skillern@lewisbrisbois.Com
Liberty Mutual Insurance Company Consolidated from 2:23-cv-525 | **Consol Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Jonathan Goins ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith Bank Of America Plaza 600 Peachtree Street Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Fax: 404-467-8845 Email:Jonathan.Goins@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000 Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com Meleah Marie Skillern ATTORNEY TO BE NOTICED

Litigants	Attorneys
	Lewis Brisbois Bisgaard & Smith 1 Gojo Plaza Ste #310 Akron, OH 44311 USA 330-272-0000 Fax: 330-272-0019 Email:Meleah.Skillern@lewisbrisbois.Com
Liberty Mutual Group Inc. Consolidated from 2:23-cv-525 | **Consol Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com
	Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com
	Jonathan Goins ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith Bank Of America Plaza 600 Peachtree Street Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Fax: 404-467-8845 Email:Jonathan.Goins@lewisbrisbois.Com
	Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com
	Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000 Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com
	Meleah Marie Skillern ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 1 Gojo Plaza Ste #310 Akron, OH 44311 USA 330-272-0000 Fax: 330-272-0019 Email:Meleah.Skillern@lewisbrisbois.Com
Liberty Mutual Plano LLC	Amber Rochelle Pickett

Litigants	Attorneys
Consolidated from 2:23-cv-525 | **Consol Defendant**	ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Jonathan Goins ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith Bank Of America Plaza 600 Peachtree Street Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Fax: 404-467-8845 Email:Jonathan.Goins@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000 Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com Meleah Marie Skillern ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 1 Gojo Plaza Ste #310 Akron, OH 44311 USA 330-272-0000 Fax: 330-272-0019 Email:Meleah.Skillern@lewisbrisbois.Com
Liberty Mutual Technology Group, Inc. Consolidated from 2:23-cv-525 | **Consol Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com

Litigants	Attorneys
	Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Jonathan Goins ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith Bank Of America Plaza 600 Peachtree Street Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Fax: 404-467-8845 Email:Jonathan.Goins@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000 Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com Meleah Marie Skillern ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 1 Gojo Plaza Ste #310 Akron, OH 44311 USA 330-272-0000 Fax: 330-272-0019 Email:Meleah.Skillern@lewisbrisbois.Com
Comparion Insurance Agency LLC Consolidated from 2:23-cv-525 | **Consol Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA

Litigants	Attorneys
	612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Jonathan Goins ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith Bank Of America Plaza 600 Peachtree Street Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Fax: 404-467-8845 Email:Jonathan.Goins@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000 Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com Meleah Marie Skillern ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 1 Gojo Plaza Ste #310 Akron, OH 44311 USA 330-272-0000 Fax: 330-272-0019 Email:Meleah.Skillern@lewisbrisbois.Com
Ironshore Holdings (U.S.) Inc. Consolidated from 2:23-cv-525 | **Consol Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Jonathan Goins ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith Bank Of America Plaza 600 Peachtree Street Ne Suite 4700

Litigants	Attorneys
	Atlanta, GA 30308 USA 404-348-8585 Fax: 404-467-8845 Email:Jonathan.Goins@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com Meleah Marie Skillern ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 1 Gojo Plaza Ste #310 Akron, OH 44311 USA 330-272-0000 Fax: 330-272-0019 Email:Meleah.Skillern@lewisbrisbois.Com
JP Morgan Chase & Co. [Terminated: 03/14/2024] **Counter Claimant**	Benjamin Hershkowitz [Terminated: 03/15/2024] Gibson Dunn & Crutcher, LLP - NYC 200 Park Ave 48th Floor New York, NY 10166-0193 USA 212-351-2410 Fax: 212-351-6210 Email:Bhershkowitz@gibsondunn.Com Katherine Dominguez [Terminated: 03/15/2024] Gibson Dunn & Crutcher, LLP - NYC 200 Park Ave 48th Floor New York, NY 10166-0193 USA 212-351-2338 Fax: 212-351-4035 Email:Kdominguez@gibsondunn.Com Melissa Richards Smith [Terminated: 03/15/2024] Gillam & Smith, LLP 303 South Washington Avenue Marshall, TX 75670 USA 903-934-8450 Fax: 903-934-9257 Email:Melissa@gillamsmithlaw.Com Nathan Robert Curtis [Terminated: 03/15/2024] Gibson, Dunn & Crutcher LLC - Dallas 2001 Ross Avenue Suite 2100 Dallas, TX 75201 USA

Litigants	Attorneys
	214-698-3423 Fax: 214-571-2961 Email:Ncurtis@gibsondunn.Com
Intellectual Ventures I LLC **Counter Defendant**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Intellectual Ventures II LLC **Counter Defendant**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Intellectual Ventures I LLC **Counter Claimant**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Intellectual Ventures II LLC **Counter Claimant**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA

Litigants	Attorneys
	650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
JP Morgan Chase & Co. [Terminated: 03/14/2024] **Counter Defendant**	Benjamin Hershkowitz [Terminated: 03/15/2024] Gibson Dunn & Crutcher, LLP - NYC 200 Park Ave 48th Floor New York, NY 10166-0193 USA 212-351-2410 Fax: 212-351-6210 Email:Bhershkowitz@gibsondunn.Com Katherine Dominguez [Terminated: 03/15/2024] Gibson Dunn & Crutcher, LLP - NYC 200 Park Ave 48th Floor New York, NY 10166-0193 USA 212-351-2338 Fax: 212-351-4035 Email:Kdominguez@gibsondunn.Com Melissa Richards Smith [Terminated: 03/15/2024] Gillam & Smith, LLP 303 South Washington Avenue Marshall, TX 75670 USA 903-934-8450 Fax: 903-934-9257 Email:Melissa@gillamsmithlaw.Com Nathan Robert Curtis [Terminated: 03/15/2024] Gibson, Dunn & Crutcher LLC - Dallas 2001 Ross Avenue Suite 2100 Dallas, TX 75201 USA 214-698-3423 Fax: 214-571-2961 Email:Ncurtis@gibsondunn.Com
Comerica Incorporated Consolidated from 2:23-cv-524 | **Counter Claimant**	Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com

Litigants

Attorneys

	Joshua S Hodas ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 633 W 5th St Suite 4000 Los Angeles, CA 90071 USA 213-680-5037 Fax: 213-250-7900 Email:Josh.Hodas@lewisbrisbois.Com
Intellectual Ventures I LLC **Counter Defendant**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Intellectual Ventures II LLC **Counter Defendant**	Jonathan Keith Waldrop LEAD ATTORNEY;ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com

Proceedings

#	Date	Proceeding Text	Source
1	11/15/2023	COMPLAINT For ***Patent*** Infringement against JP Morgan Chase & Co. (Filing fee $ 402 receipt number ATXEDC-9818670.), filed by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Civil Cover Sheet, # 2 Exhibit 1 - US8332844, # 3 Exhibit 2 - US8407722, # 4 Exhibit 3 - US7280998B1, # 5 Exhibit 4 - US7712080B2, # 6 Exhibit 5 - US7314167, # 7 Exhibit 6 - US7949785, # 8 Exhibit 7 - Notice Letter, # 9 Exhibit 8 - '844 Chart, # 10 Exhibit 9 - '722 Chart, # 11 Exhibit 10 - '998 Chart, # 12 Exhibit 11 - '080 Chart, # 13 Exhibit 12 - '167 Chart, # 14 Exhibit 13 - '785 Chart)(Gardner, Allen) (Entered: 11/15/2023)	
2	11/15/2023	Notice of Filing of ***Patent***/Trademark Form (AO 120). AO 120	

#	Date	Proceeding Text	Source
		mailed to the Director of the U.S. ***Patent*** and Trademark Office. (Attachments: # 1 Additional Attachment(s))(Gardner, Allen) (Entered: 11/15/2023)	
3	11/15/2023	Fed. R. Civ. P. 7.1(a)(1) Disclosure Statement filed by Intellectual Ventures I LLC, Intellectual Ventures II LLC (Gardner, Allen) (Entered: 11/15/2023)	
4	11/15/2023	DEMAND for Trial by Jury by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Gardner, Allen) (Entered: 11/15/2023)	
	11/15/2023	District Judge Rodney Gilstrap added. (klc,) (Entered: 11/15/2023)	
	11/15/2023	In accordance with the provisions of 28 USC Section 636(c), you are hereby notified that a U.S. Magistrate Judge of this district court is available to conduct any or all proceedings in this case including a jury or non-jury trial and to order the entry of a final judgment. The form Consent to Proceed Before Magistrate Judge is available on our website. All signed consent forms, excluding pro se parties, should be filed electronically using the event Notice Regarding Consent to Proceed Before Magistrate Judge. (klc,) (Entered: 11/15/2023)	
5	11/15/2023	SUMMONS Issued as to JP Morgan Chase & Co. c/o C T Corporation System. (nkl,) (Entered: 11/15/2023)	
6	11/20/2023	SUMMONS Returned Executed by Intellectual Ventures I LLC, Intellectual Ventures II LLC. JP Morgan Chase & Co. served on 11/17/2023. (Gardner, Allen) (Entered: 11/20/2023)	
7	12/05/2023	MOTION for Extension of Time to File Answer re 1 Complaint,, by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order)(Waldrop, Jonathan) (Entered: 12/05/2023)	
8	12/08/2023	ORDER granting 7 Motion for Extension of Time to Answer re 7 MOTION for Extension of Time to File Answer re 1 Complaint,, . Signed by District Judge Rodney Gilstrap on 12/8/2023. (klc,) (Entered: 12/08/2023)	
9	01/05/2024	NOTICE of Attorney Appearance by Benjamin Hershkowitz on behalf of JP Morgan Chase & Co. (Hershkowitz, Benjamin) (Entered: 01/05/2024)	
10	01/05/2024	JOINT MOTION Regarding Stipulation For Dismissal Of JPMorgan Chase & Co. And Substitution Of JPMorgan Chase Bank, National Association by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order)(Waldrop, Jonathan) (Entered: 01/05/2024)	
11	01/09/2024	NOTICE of Attorney Appearance by Melissa Richards Smith on behalf of JP Morgan Chase & Co. (Smith, Melissa) (Entered: 01/09/2024)	
12	01/09/2024	UNOPPOSED MOTION for Extension of Time to File Answer by JP Morgan Chase & Co.. (Attachments: # 1 Proposed Order)(Smith, Melissa) (Entered: 01/09/2024)	
13	01/19/2024	ORDER granting 12 Motion for Extension of Time to Answer re 12 UNOPPOSED MOTION for Extension of Time to File Answer JP Morgan Chase & Co. answer due 1/22/2024. Signed by District Judge Rodney Gilstrap on 1/19/2024. (ch,) (Entered: 01/22/2024)	
14	01/22/2024	NOTICE of Attorney Appearance by Katherine Dominguez on behalf of JP Morgan Chase & Co. (Dominguez, Katherine) (Entered: 01/22/2024)	
15	01/22/2024	NOTICE of Attorney Appearance by Nathan Robert Curtis on behalf of JP Morgan Chase & Co. (Curtis, Nathan) (Entered: 01/22/2024)	
16	01/22/2024	ANSWER to 1 Complaint,, , COUNTERCLAIM against Intellectual	

#	Date	Proceeding Text	Source
		Ventures I LLC, Intellectual Ventures II LLC by JP Morgan Chase & Co..(Hershkowitz, Benjamin) (Entered: 01/22/2024)	
17	01/22/2024	Fed. R. Civ. P. 7.1(a)(1) Disclosure Statement filed by JP Morgan Chase & Co. identifying Other Affiliate JPMorgan Chase Bank, National Association, Interested Party Vanguard Group, Inc. for JP Morgan Chase & Co., JP Morgan Chase & Co.. (Hershkowitz, Benjamin) (Entered: 01/22/2024)	
18	01/26/2024	NOTICE of Readiness for Scheduling Conference by Intellectual Ventures I LLC, Intellectual Ventures II LLC (Gardner, Allen) (Entered: 01/26/2024)	
19	02/12/2024	ANSWER to 16 Answer to Complaint, Counterclaim , COUNTERCLAIM against JP Morgan Chase & Co. by Intellectual Ventures I LLC, Intellectual Ventures II LLC.(Waldrop, Jonathan) (Entered: 02/12/2024)	
20	02/13/2024	CONSOLIDATION ORDER - The above-captioned cases are hereby ORDERED to be CONSOLIDATED for all pretrial issues with the LEAD CASE, Case No. 2:23-cv-00523. All parties are instructed to file any future filings in the LEAD CASE. Individual cases remain active for trial. Signed by District Judge Rodney Gilstrap on 2/13/2024. (ch,) (Entered: 02/13/2024)	
21	02/14/2024	SCHEDULING ORDER: Scheduling/Case Management Conference set for 3/25/2024 at 10:00 AM before District Judge Rodney Gilstrap.. Signed by District Judge Rodney Gilstrap on 2/14/2024. (ch,) (Entered: 02/14/2024)	
22	02/16/2024	Comerica's ANSWER to Complaint in Member Case 2:23-0524, COUNTERCLAIM against All Plaintiffs by Comerica Incorporated.(Curry, Joshua) (Entered: 02/16/2024)	
23	02/22/2024	UNOPPOSED MOTION for Discovery To Allow Limited Discovery As To Venue Issues And For An Extension Of The Briefing Deadlines Accordingly by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order)(Waldrop, Jonathan) (Entered: 02/22/2024)	
24	03/01/2024	ORDER granting 23 UNOPPOSED MOTION for Discovery To Allow Limited Discovery As To Venue Issues And For An Extension Of The Briefing Deadlines Accordingly. Signed by District Judge Rodney Gilstrap on 4/1/2024. (ch,) (Entered: 03/01/2024)	
25	03/06/2024	NOTICE of Attorney Appearance by Joshua S Hodas on behalf of Comerica Incorporated, Comparion Insurance Agency LLC, Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. (Hodas, Joshua) (Entered: 03/06/2024)	
26	03/08/2024	ANSWER to 22 Answer to Complaint, Counterclaim by Intellectual Ventures I LLC, Intellectual Ventures II LLC.(Waldrop, Jonathan) (Entered: 03/08/2024)	
27	03/08/2024	JOINT MOTION for Extension of Time to File Infringement Contentions by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order)(Waldrop, Jonathan) (Entered: 03/08/2024)	
28	03/13/2024	NOTICE of Attorney Appearance by Meleah Marie Skillern on behalf of Comparion Insurance Agency LLC, Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. (Skillern, Meleah) (Entered: 03/13/2024)	
29	03/14/2024	ORDER granting 10 Motion Regarding Stipulation for Dismissal of JPMorgan Chase & Co. and Substitution of JP Morgan Chase Bank, National Association. Court ORDERS that JP Morgan	

#	Date	Proceeding Text	Source
		Chase & Co. is DISMISSED from the above-captioned action, and JP Morgan Chase Bank, National Association shall be substituted as a Defendant in this action. The Court further ORDERS that hereinafter the case caption shall reflect the name of the new, substituted Defendantnamely, JP Morgan Chase Bank, National Association.. Signed by District Judge Rodney Gilstrap on 3/14/2024. (ch,) (Entered: 03/14/2024)	
30	03/15/2024	ORDER granting 27 JOINT MOTION for Extension of Time to File Infringement Contentions. Signed by District Judge Rodney Gilstrap on 3/15/2024. (ch,) (Entered: 03/18/2024)	
31	03/21/2024	NOTICE of Attorney Appearance by Melissa Richards Smith on behalf of JP Morgan Chase Bank, National Association (Smith, Melissa) (Entered: 03/21/2024)	
32	03/22/2024	NOTICE OF COMPLIANCE by Intellectual Ventures I LLC, Intellectual Ventures II LLC Regarding Service Of Infringement Contentions (Waldrop, Jonathan) (Entered: 03/22/2024)	
	03/25/2024	Minute Entry for proceedings held before District Judge Rodney Gilstrap (Lead 2:23-cv-523 and Member 2:23-cv-524 and 2:23-cv-525): Scheduling Conference/Case Management Conference held on 3/25/2024. Counsel for the parties appeared. Court asked whether they consented to trial before the U.S. Magistrate Judge. Court proceeded to give counsel Claim Construction and Jury Selection/Trial dates. (Court Reporter Shawn McRoberts) (aeb) (Entered: 03/26/2024)	
33	03/26/2024	***FILED IN ERROR PER ATTORNEY***NOTICE of Attorney Appearance by Jonathan Goins on behalf of Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. (Goins, Jonathan) Modified on 3/27/2024 (CH). (Entered: 03/26/2024)	
34	03/26/2024	NOTICE of Attorney Appearance by Francois Ecclesiaste on behalf of Comerica Incorporated, Comparion Insurance Agency LLC, Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. (Ecclesiaste, Francois) (Entered: 03/26/2024)	
35	03/27/2024	NOTICE of Attorney Appearance by Jonathan Goins on behalf of Comparion Insurance Agency LLC, Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. (Goins, Jonathan) (Entered: 03/27/2024)	
36	04/02/2024	MOTION to Stay and Joint Notice of Settlement by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Waldrop, Jonathan) (Entered: 04/02/2024)	
37	04/05/2024	ORDER granting 36 MOTION to Stay and Joint Notice of Settlement. Signed by District Judge Rodney Gilstrap on 5/4/2024. (CH) (Entered: 04/05/2024)	
38	04/08/2024	JOINT MOTION for Entry of Docket Control Order by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order - Docket Control Order)(Waldrop, Jonathan) (Entered: 04/08/2024)	
39	04/08/2024	JOINT MOTION for Entry of Discovery Order by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order - Discovery Order)(Waldrop, Jonathan) (Entered: 04/08/2024)	
40	04/11/2024	DOCKET CONTROL ORDER granting 38 JOINT MOTION for Entry of Docket Control Order. (Pretrial Conference set for 6/16/2025 at 09:00 AM before Magistrate Judge Roy S. Payne.,	

#	Date	Proceeding Text	Source
		Jury Selection set for 7/21/2025 at 09:00AM before District Judge Rodney Gilstrap., Markman Hearing set for 2/4/2025 at 09:00 AM before Magistrate Judge Roy S. Payne.). Signed by District Judge Rodney Gilstrap on 4/11/2024. (CH) (Entered: 04/11/2024)	
41	04/11/2024	DISCOVERY ORDER granting 39 JOINT MOTION for Entry of Discovery Order. Signed by District Judge Rodney Gilstrap on 4/11/2024. (CH) (Entered: 04/11/2024)	
42	04/12/2024	FIRST AMENDED DOCKET CONTROL ORDER granting FIRST AMENDED DOCKET CONTROL ORDER (Markman Hearing set for 1/21/2025 at 09:00 AM before District Judge Rodney Gilstrap.. Signed by District Judge Rodney Gilstrap on 4/12/2024. (CH) (Entered: 04/12/2024)	
43	04/15/2024	JOINT MOTION To Amend The Docket Control Order To Extend Time To File Protective Order by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order)(Waldrop, Jonathan) (Entered: 04/15/2024)	
44	04/15/2024	NOTICE of Discovery Disclosure by Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. re Initial and Additional Disclosures (Ecclesiaste, Francois) (Entered: 04/15/2024)	
45	04/15/2024	NOTICE of Discovery Disclosure by Comerica Incorporated re Initial and Additional Disclosures (Ecclesiaste, Francois) (Entered: 04/15/2024)	
46	04/16/2024	NOTICE of Discovery Disclosure by Intellectual Ventures I LLC, Intellectual Ventures II LLC re Service of Initial and Additional Disclosures on Comerica Incorporated (Waldrop, Jonathan) (Entered: 04/16/2024)	
47	04/16/2024	NOTICE of Discovery Disclosure by Intellectual Ventures I LLC, Intellectual Ventures II LLC re Service of Initial and Additional Disclosures on Liberty Mutual Holding Company Inc., et al. (Waldrop, Jonathan) (Entered: 04/16/2024)	
	04/17/2024	SEE ORDER 42 Pretrial Conference set for 6/16/2025 at 09:00 AM before District Judge Rodney Gilstrap. (KLC) (Entered: 04/17/2024)	
48	04/23/2024	ORDER granting 43 JOINT MOTION To Amend The Docket Control Order To Extend Time To File Protective Order. Signed by District Judge Rodney Gilstrap on 4/23/2024. (CH) (Entered: 04/23/2024)	
49	04/23/2024	JOINT MOTION for Protective Order by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order)(Waldrop, Jonathan) (Entered: 04/23/2024)	
50	04/29/2024	AGREED PROTECTIVE ORDER. Signed by District Judge Rodney Gilstrap on 04/29/2024. (KLC) (Entered: 04/29/2024)	
51	05/13/2024	JOINT MOTION to Dismiss by JP Morgan Chase Bank, National Association. (Attachments: # 1 Proposed Order)(Smith, Melissa) (Entered: 05/13/2024)	
52	05/17/2024	ORDER granting 51 JOINT MOTION to Dismiss JP Morgan Chase Bank, National Association. Court ACCEPTS AND ACKNOWLEDGES that all claims and causes of action asserted in Lead Case No. 2:23-cv-523 are DISMISSED WITH PREJUDICE (Motion(s) 51 terminated). Signed by District Judge Rodney Gilstrap on 5/17/2024. (CH) (Entered: 05/17/2024)	

Patents

Number	Title	Issued	Class	Subclass

Number	Title	Issued	Class	Subclass
7,712,080	Systems and methods for parallel distributed programming	05/04/2010	717	119
7,949,785	Secure virtual community network system	05/24/2011	709	245
8,407,722	Asynchronous messaging using a node specialization architecture in the dynamic routing network	03/26/2013	719	316

Copyright © LexisNexis CourtLink, Inc. All Rights Reserved.
*** THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY ***

End of Document

User Name: Patricia Martin
Date and Time: Monday, June 3, 2024 4:04:00PM EDT
Job Number: 225730853

Document (1)

1. 2:23cv625, Intellectual Ventures I Llc Et Al V. Liberty Mutual Holding Company Inc. Et Al., Pursuant To Court Order, Docket In The Lead Case As Directed

Client/Matter: -None-
Search Terms: 7949785 or 7,949,785
Search Type: Terms and Connectors
Narrowed by:

Content Type	Narrowed by
Dockets	Case Status: Open,Unknown,Closed; Case Type: Civil

LexisNexis | About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2024 LexisNexis

2:23cv525, Intellectual Ventures I Llc Et Al V. Liberty Mutual Holding Company Inc. Et Al Pursuant To Court Order, Docket In The Lead Case As Directed

US District Court Docket

United States District Court, Texas Eastern

(Marshall)

This case was retrieved on 06/02/2024

Header

Case Number: 2:23cv525
Date Filed: 11/15/2023
Assigned To: District Judge Rodney Gilstrap
Nature of Suit: ***Patent*** (830)
Cause: ***Patent*** Infringement
Lead Docket: 2:23cv00523
Other Docket: None
Jurisdiction: Federal Question

Class Code: Open
Statute: 15:1126
Jury Demand: Plaintiff
Demand Amount: $0
NOS Description: ***Patent***

Participants

Litigants	Attorneys
Intellectual Ventures I LLC **Plaintiff**	Jonathan Keith Waldrop ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Intellectual Ventures II LLC **Plaintiff**	Jonathan Keith Waldrop ATTORNEY TO BE NOTICED Kasowitz Benson Torres LLP - Redwood Shores 333 Twin Dolphin Drive, Suite 200 Redwood Shores, CA 94065 USA 650-453-5425 Fax: 650-453-5171 Email:Jwaldrop@kasowitz.Com

Patricia Martin

Litigants	Attorneys
	Allen Franklin Gardner ATTORNEY TO BE NOTICED Allen Gardner Law, PLLC 609 South Fannin Tyler, TX 75701 USA 903-944-7537 Fax: 903-944-7856 Email:Allen@allengardnerlaw.Com
Liberty Mutual Holding Company Inc. **Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com
Liberty Mutual Insurance Company **Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com

Litigants	Attorneys
Liberty Mutual Group Inc. **Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com
Liberty Mutual Plano LLC **Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com
Liberty Mutual Technology Group, Inc. **Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com

Litigants	Attorneys
	Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com
Comparion Insurance Agency LLC **Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048 Email:Francois.Ecclesiaste@lewisbrisbois.Com Joshua David Curry ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith 600 Peachtree Street, Ne Suite 4700 Atlanta, GA 30308 USA 404-348-8585 Email:Josh.Curry@lewisbrisbois.Com
Ironshore Holdings (U.S.) Inc. **Defendant**	Amber Rochelle Pickett ATTORNEY TO BE NOTICED Lewis Brisbois Bisgaard & Smith LLP - Dallas 2100 Ross Avenue Suite 2000 Dallas, TX 75201 USA 214-722-7100 Fax: 214-722-7111 Email:Amber.Pickett@lewisbrisbois.Com Francois Ecclesiaste ATTORNEY TO BE NOTICED Lewis Brisbois 90 South 7th Street Ste 2800 Minneapolis, MN 55402 USA 612-428-5048

Litigants

Attorneys

Email:Francois.Ecclesiaste@lewisbrisbois.Com

Joshua David Curry
ATTORNEY TO BE NOTICED
Lewis Brisbois Bisgaard & Smith
600 Peachtree Street, Ne Suite 4700
Atlanta, GA 30308
USA
404-348-8585 Email:Josh.Curry@lewisbrisbois.Com

Proceedings

#	Date	Proceeding Text	Source
1	11/15/2023	COMPLAINT For ***Patent*** Infringement against All Defendants (Filing fee $ 402 receipt number ATXEDC-9818700.), filed by Intellectual Ventures II LLC, Intellectual Ventures I LLC. (Attachments: # 1 Civil Cover Sheet, # 2 Exhibit 1 - US8332844, # 3 Exhibit 2 - US8407722, # 4 Exhibit 3 - US7712080B2, # 5 Exhibit 4 - US7949785, # 6 Exhibit 5 - Notice Letter, # 7 Exhibit 6 - '844 Chart, # 8 Exhibit 7 - '722 Chart, # 9 Exhibit 8 - '080 Chart, # 10 Exhibit 9 - '785 Chart)(Gardner, Allen) (Entered: 11/15/2023)	
2	11/15/2023	Notice of Filing of ***Patent***/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. ***Patent*** and Trademark Office. (Gardner, Allen) (Entered: 11/15/2023)	
3	11/15/2023	Fed. R. Civ. P. 7.1(a)(1) Disclosure Statement filed by Intellectual Ventures I LLC, Intellectual Ventures II LLC (Gardner, Allen) (Entered: 11/15/2023)	
4	11/15/2023	DEMAND for Trial by Jury by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Gardner, Allen) (Entered: 11/15/2023)	
	11/15/2023	District Judge Rodney Gilstrap added. (klc,) (Entered: 11/15/2023)	
	11/15/2023	In accordance with the provisions of 28 USC Section 636(c), you are hereby notified that a U.S. Magistrate Judge of this district court is available to conduct any or all proceedings in this case including a jury or non-jury trial and to order the entry of a final judgment. The form Consent to Proceed Before Magistrate Judge is available on our website. All signed consent forms, excluding pro se parties, should be filed electronically using the event Notice Regarding Consent to Proceed Before Magistrate Judge. (klc,) (Entered: 11/15/2023)	
5	11/15/2023	SUMMONS Issued as to Comparion Insurance Agency LLC, Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc.. (Attachments: # 1 Additional Attachment(s), # 2 Additional Attachment(s), # 3 Additional Attachment(s), # 4 Additional Attachment(s), # 5 Additional Attachment(s), # 6 Additional Attachment(s))(ch,) (Entered: 11/15/2023)	
6	11/22/2023	SUMMONS Returned Executed by Intellectual Ventures II LLC, Intellectual Ventures I LLC. Comparion Insurance Agency LLC served on 11/20/2023; Ironshore Holdings (U.S.) Inc. served on 11/20/2023; Liberty Mutual Group Inc. served on 11/20/2023; Liberty Mutual Holding Company Inc. served on 11/20/2023; Liberty Mutual Insurance Company served on 11/20/2023; Liberty Mutual Plano LLC served on 11/20/2023; Liberty Mutual	

#	Date	Proceeding Text	Source
		Technology Group, Inc. served on 11/20/2023. (Attachments: # 1 Additional Attachment(s) Comparion Summons Return, # 2 Additional Attachment(s) Ironshore Summons Return, # 3 Additional Attachment(s) Liberty Mutual Group Summons Return, # 4 Additional Attachment(s) Liberty Mutual Holdings Summons Return, # 5 Additional Attachment(s) Liberty Mutual Plano Summons Return, # 6 Additional Attachment(s) Liberty Mutual Tech Summons Return)(Gardner, Allen) (Entered: 11/22/2023)	
7	12/06/2023	Defendant's Unopposed First Application for Extension of Time to Answer Complaint re Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc..(Pickett, Amber) (Entered: 12/06/2023)	
	12/06/2023	Defendant's Unopposed FIRST Application for Extension of Time to Answer Complaint is granted pursuant to Local Rule CV-12 for Liberty Mutual Plano LLC to 1/25/2024; Liberty Mutual Holding Company Inc. to 1/25/2024; Liberty Mutual Technology Group, Inc. to 1/25/2024; Ironshore Holdings (U.S.) Inc. to 1/25/2024; Liberty Mutual Insurance Company to 1/25/2024; Liberty Mutual Group Inc. to 1/25/2024. 45 Days Granted for Deadline Extension.(ch,) (Entered: 12/06/2023)	
8	01/24/2024	Defendant's Unopposed First Application for Extension of Time to Answer Complaint re Comparion Insurance Agency LLC.(Pickett, Amber) (Entered: 01/24/2024)	
	01/24/2024	Defendant's Unopposed FIRST Application for Extension of Time to Answer Complaint is granted pursuant to Local Rule CV-12 for Comparion Insurance Agency LLC to 1/25/2024. 45 Days Granted for Deadline Extension.(ch,) (Entered: 01/24/2024)	
9	01/25/2024	MOTION to Dismiss For Improper Venue by Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc.. (Attachments: # 1 Exhibit Exhibit A in Support of Liberty Mutual Defendants' Motion to Dismiss for Improper Venue)(Curry, Joshua) (Entered: 01/25/2024)	
10	01/25/2024	Fed. R. Civ. P. 7.1(a)(1) Disclosure Statement filed by Comparion Insurance Agency LLC, Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. (Curry, Joshua) (Entered: 01/25/2024)	
11	01/30/2024	NOTICE of Readiness for Scheduling Conference by Intellectual Ventures I LLC, Intellectual Ventures II LLC (Waldrop, Jonathan) (Entered: 01/30/2024)	
12	02/01/2024	UNOPPOSED MOTION for Extension of Time to File Response/Reply as to 9 MOTION to Dismiss For Improper Venue by Intellectual Ventures I LLC, Intellectual Ventures II LLC. (Attachments: # 1 Proposed Order)(Waldrop, Jonathan) (Entered: 02/01/2024)	
13	02/10/2024	ORDER granting 12 UNOPPOSED MOTION for Extension of Time to File Response/Reply as to 9 MOTION to Dismiss For Improper Venue , 9 MOTION to Dismiss For Improper Venue Responses due by 2/23/2024. Signed by District Judge Rodney Gilstrap on 2/10/2024. (ch,) (Entered: 02/12/2024)	
14	02/13/2024	CONSOLIDATION ORDER - The above-captioned cases are hereby ORDERED to be CONSOLIDATED for all pretrial issues with the LEAD CASE, Case No. 2:23-cv-00523. All parties are instructed to file any future filings in the LEAD CASE. Individual	

#	Date	Proceeding Text	Source
		cases remain active for trial. Signed by District Judge Rodney Gilstrap on 2/13/2024. (ch,) (Entered: 02/13/2024)	
15	03/26/2024	***FILED IN ERROR PER ATTORNEY*** NOTICE of Attorney Appearance by Francois Ecclesiaste on behalf of Comparion Insurance Agency LLC, Ironshore Holdings (U.S.) Inc., Liberty Mutual Group Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Insurance Company, Liberty Mutual Plano LLC, Liberty Mutual Technology Group, Inc. (Ecclesiaste, Francois) Modified on 3/26/2024 (CH). (Entered: 03/26/2024)	

Patents

Number	Title	Issued	Class	Subclass
7,712,080	Systems and methods for parallel distributed programming	05/04/2010	717	119
7,949,785	Secure virtual community network system	05/24/2011	709	245
8,407,722	Asynchronous messaging using a node specialization architecture in the dynamic routing network	03/26/2013	719	316

Copyright © LexisNexis CourtLink, Inc. All Rights Reserved.
*** THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY ***

End of Document

☐ US7949785B2 - Secure virtual community network system

Original

Bibliographic information & Images

Publication number and date
US7949785B2
2011-05-24

Granted

Application number and date
US10403818 (/api/control?client=&query=AN:("US10403818")&autosearch=true)
2003-03-31

Priority number and date
US10403818 (/api/control?client=&query=PRN:("US10403818")&autosearch=true)
2003-03-31

Ultimate owner
F. Poszat Hu (/api/control?client=&query=uo:("F.%20Poszat%20Hu")&autosearch=true)

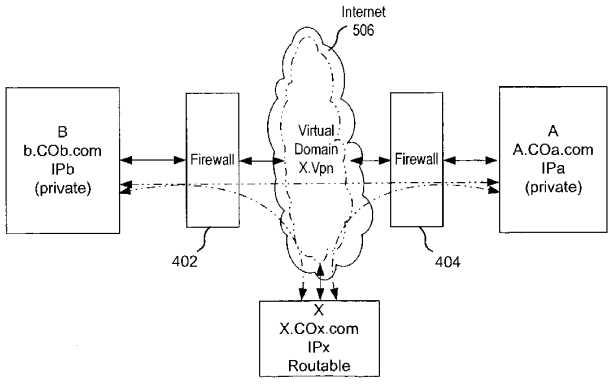
Original assignee
Hasan S. Alkhatib (/api/control?client=&query=pa:("Hasan%20S.%20Alkhatib")&autosearch=true)

Current assignee
INPRO NETWORK FACILITY, LLC (/api/control?client=&query=pacu:("INPRO%20NETWORK%20FACILITY%2C%20LLC")&autosearch=true)

Inventor
Hasan S. Alkhatib (/api/control?client=&query=in:("Hasan%20S.%20Alkhatib")&autosearch=true)

Legal representative
McAndrews, Held & Malloy, Ltd. (/api/control?client=&query=ag:("McAndrews%2C%20Held%20%26%20Malloy%2C%20Ltd.")&autosearch=true)

1/22 Clipped image



Abstract

A private virtual dynamic network is provided for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. In one embodiment, the present invention provides a separate private virtual address realm, seen to each user as a private network, while seamlessly crossing public and private network boundaries. One implementation of the present invention uses an agent to enable an entity to participate in the network without requiring the member to add new hardware or software.

Original

Claims

1. A virtual network system, comprising: a virtual network manager implemented with a first device memory and a first device processor of a first computing device, the virtual network manager configured to register devices in a virtual network that is defined by a domain name, each device in the virtual network being identified to the other devices by a virtual network address that is unique for each device and not directly routable via a public

AA/SWA Ex. 1015, p.429 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

network, the virtual network manager further configured to distribute a virtual network address to a device when the device is registered in the virtual network; a route director implemented with a second device memory and a second device processor of a second computing device, the route director configured to communicate data between the devices that are registered in the virtual network, the data being communicated as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device; and the virtual network manager further configured to receive a DNS request from the source device, and return a public network address of the route director, a private network address for the destination device, and the second virtual network address that corresponds to the destination device.

2. The system of claim 1 wherein each of the devices communicate with the virtual network manager and the other devices in the virtual network via an associated agent.

3. The system of claim 2 wherein the associated agent is installed on a proxy device which is a proxy agent for one or more of the devices in the virtual network with respect to the virtual network manager and the route director.

4. The system of claim 2 wherein the virtual network manager is further configured to: receive a request from the agent associated with a device in a private network to register the device in the virtual network; and detect a presence of a NAT device via which the request is routed from the agent to the virtual network manager.

5. The system of claim 4 wherein the virtual network manager is further configured to receive the request from the agent as a message, and detect the presence of the NAT device by comparing a field in a payload of the message with a source address in a header of the message.

6. The system of claim 1 wherein each of the devices include an agent configured to communicate with the virtual network manager and agents of the other devices in the virtual network.

7. The system of claim 1 wherein the virtual network manager is coupled to the public network and has an associated public network address.

8. The system of claim 1 wherein the route director is further configured to receive the encapsulated packets when routed to a public network address corresponding to the route director.

9. The system of claim 1 wherein each of the devices in the virtual network are further identified by at least one physical network address.

10. The system of claim 9 wherein the physical network addresses that are associated with the devices in the virtual network are dynamic.

11. The system of claim 9 wherein the physical network addresses that are associated with the devices in the virtual network are static.

12. The system of claim 9 wherein the physical network addresses that are associated with the devices in the virtual network are private network addresses, and wherein the virtual network addresses are unique in the virtual network so as not to conflict with the private network addresses.

13. The system of claim 9 wherein the source device is coupled to a first private network and accesses a public network via a first NAT device configured to transmit the encapsulated packets, an encapsulated packet further including the physical network address of the source device as a private network address in the first private network.

14. The system of claim 13 wherein the physical network address of the source device is dynamic.

15. The system of claim 13 wherein the physical network address of the source device is static.

16. The system of claim 13 wherein the destination device is coupled to a second private network and accesses the public network via a second NAT device, the encapsulated packet further including the physical network address of the destination device as a private network address in the second private network.

17. The system of claim 16 wherein the physical network address of the destination device is dynamic.

18. The system of claim 16 wherein the physical network address of the destination device is static.

19. The system of claim 16 wherein said first private network and said second private network share at least one network address.

20. The system of claim 1 wherein the route director is further configured to: provide a device-specific pseudo address assignment for the device in the virtual network when the device communicates with the route director via a NAT device; and store an association of the device-specific pseudo address with a public network address of the NAT device and a port number of the NAT device.

21. The system of claim 1 wherein the route director includes a translator for virtual network address information for a device in the virtual network that is implemented in a private network.

22. The system of claim 1 wherein the virtual network manager is coupled to the public network and includes a public network address.

23. The system of claim 22 wherein the route director is coupled to the public network and includes a different public network address than the public network address of the virtual network manager.

24. The system of claim 22 wherein the route director is coupled to a private network and includes a private network address.

25. The system of claim 1 wherein the encapsulated packets further include virtual IP packets configured for communication of the data, the virtual IP packets being encrypted prior to being encapsulated.

26. The system of claim 25 wherein the virtual IP packets are encrypted using IPSEC.

27. The system of claim 25 wherein the virtual IP packets are encrypted using DES or triple DES.

28. The system of claim 1 wherein the virtual network manager includes a virtual community definition that is defined by the domain name, and includes one or more of the devices that are registered in the virtual network.

29. The system of claim 1 wherein the route director is a public route director in the public network, the system further comprising a private route director in a private network configured to enable access to devices of the private network that are also in the virtual network from devices of the public network that are also in the virtual network.

30. A virtual network manager, comprising: a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address; a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to: receive a registration request from an agent associated with a device; distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.

AA/SWA Ex. 1015, p.430 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

31. The virtual network manager of claim 30 further comprising an additional network interface configured for data communication via a public network.

32. The virtual network manager of claim 31 wherein the network interface is a UDP port configured for data communication via the virtual network, and wherein the additional network interface is a TCP port configured for registration communications via the public network.

33. The virtual network manager of claim 30 wherein the network interface is a UDP port configured for data communication via the virtual network.

34. The virtual network manager of claim 30 wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network.

35. The virtual network manager of claim 30 further comprising a join module configured to receive a join request from the agent associated with the device to indicate that the device is connected for data communication within the virtual network, the join module further configured to receive a leave request from the agent associated with the device to indicate that the device will be disconnected from data communication within the virtual network.

36. The virtual network manager of claim 35 wherein the join module is further configured to provide virtual network addresses to the devices that are registered in the virtual network.

37. The virtual network manager of claim 35 wherein the join module is further configured to maintain data to associate a virtual network address with a device in the virtual network.

38. A virtual network system, comprising: a computing device that includes at least a memory and a processor configured to implement a network manager of a virtual network that is defined by a public domain name, the network manager configured to distribute virtual network addresses to devices that register as members in the virtual network, each device in the virtual network being identified to the other devices by a virtual network address associated with the device; a first virtual network agent associated with a first device that is registered as a member in the virtual network; at least a second virtual network agent associated with at least a second device that is registered as a member in the virtual network; a route director configured to route communications between the first device and the at least second device in the virtual network via the respective first and second virtual network agents, the communications configured for routing as encapsulated packets that include a first virtual network address that is not directly routable corresponding to the first device and a second virtual network address that is not directly routable corresponding to the at least second device; and the network manager includes a DNS server configured to provide authoritative responses for DNS queries in the virtual network, the DNS server further configured to receive a DNS query from the first device and return a network address of the route director, a network address of the second device, and the virtual network address of the second device.

39. The system of claim 38 wherein the route director is a public network route director that includes a public network interface and the network address is a public network address by which the first and second virtual network agents communicate with the public network route director.

40. The system of claim 38 wherein the route director is a private route director that includes a private physical network interface and the network address is a private physical network address.

41. The system of claim 38 wherein the first virtual network agent is installed on the first device for data communication via the virtual network.

42. The system of claim 41 wherein the first device is in a private physical network, has an associated private network address, and has the associated virtual network address that is not directly routable by which the first device can be identified by the at least second virtual network agent from outside of the private physical network.

43. The system of claim 41 wherein the first device is coupled to a public physical network, has an associated public network address, and has the associated virtual network address by which the first device can be identified by the at least second virtual network agent.

44. The system of claim 38 wherein the first virtual network agent is a proxy agent for the first device with respect to the network manager and the route director.

45. The system of claim 38 wherein the first and second devices are configured to access the virtual network from separate private address physical realms.

46. The system of claim 38 wherein the network manager includes at least a first community definition and a second community definition, the first community definition being defined by the public domain name and includes one or more of the devices that are registered in the virtual network, and the second community definition being defined by a different public domain name and includes one or more different devices that are registered in the virtual network.

47. The system of claim 38 wherein the network manager includes a member authenticator configured to authenticate the devices that request to register with the network manager.

48. A computer-implemented method, comprising: receiving registration requests from devices that request to be registered as members of a virtual network that is defined by a domain name having an associated public network address in a public network, each of the devices having an associated private network address; distributing a virtual network address to a device to register the device as a member in the virtual network, each device in the virtual network being identified to the other devices by the virtual network address that is associated with the device; routing communications between the devices that are registered in the virtual network, the communications being routed as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device; and transmitting a response to a DNS request received from one of the devices that are the members in the virtual network, the response to the DNS request including a public network address of a route director that registers the devices, a public network address of the destination device, and the second virtual network address that corresponds to the destination device.

49. The method of claim 48 further comprising providing the devices in the virtual network with a communication agent.

50. The method of claim 49 wherein said providing the devices in the virtual network with a communication agent includes providing a proxy agent.

51. The method of claim 48 further comprising authenticating the devices as the members in the virtual network.

52. The method of claim 48 further comprising defining a member set of the virtual network that includes one or more of the devices, and assigning the domain name that defines the virtual network.

53. The method of claim 48 further comprising defining at least two member sets of the virtual network that each include one or more of the devices, the at least two member sets having at least one different device.

54. The method of claim 48 further comprising assigning the virtual network address to the device as an IPV4 compliant address.

55. The method of claim 54 wherein the IPV4 compliant address is non-routable.

56. The method of claim 48 further comprising routing network traffic via the public network from a first device having a public network address to a second device having a different public network address, the network traffic being routed as data packets having a source address which is the virtual

AA/SWA Ex. 1015, p.431 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

network address of the first device and a destination address which is the virtual network address of the second device, the data packets being encapsulated to include a second source address which is a public network address of the first device and a second destination address which is the different public network address of the second device.

57. The method of claim 48 further comprising routing network traffic from a first device in a private physical network having a private network address to a second device having a public network address, the network traffic being routed as data packets having a source address which is the virtual network address of the first device, a destination address which is the virtual network address of the second device, and a shim which includes the private network address, the data packets being encapsulated to include a second destination address which is the public network address of the second device.

58. The method of claim 48 further comprising routing network traffic from a first device in a private physical network having a first private network address to a second device in a different private physical network having a second private network address, the network traffic being routed as encapsulated packets having a source address which is the virtual network address of the first device, a destination address which is the virtual network address of the second device, and a shim which includes the first and second private network addresses.

59. The method of claim 58 wherein the first private network address and the second private network address are identical.

60. The method of claim 48 further comprising: receiving a join status request from a first device in the virtual network as a query to determine the status of a second device in the virtual network; and responding to the join status request to indicate whether or not the second device is joined to the virtual network for data communication.

61. The method of claim 48 further comprising applying a group policy to the devices that are registered as the members of the virtual network.

62. One or more processor readable storage media devices comprising processor readable code that, if executed by a computer device, implements a virtual network manager to: receive registration requests from devices that request to be registered as members of a virtual network that is defined by a domain name having an associated public network address in a public network, each of the devices having an associated private network address; distribute a virtual network address to a device to register the device as a member in the virtual network, each device in the virtual network being identified to the other devices by the virtual network address that is associated with the device; manage communications routed between the devices that are registered in the virtual network, the communications routed as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device; and transmit a response to a DNS request received from one of the devices that are the members in the virtual network, the response to the DNS request including a public network address of the virtual network manager, a public network address of the destination device, and the second virtual network address that corresponds to the destination device.

63. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to provide the devices in the virtual network with a communication agent.

64. One or more processor readable storage media devices as recited in claim 63 wherein the virtual network manager provides the as a proxy agent.

65. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to define a member set of the virtual network that includes one or more of the devices, and the domain name that defines the virtual network.

66. One or more processor readable storage media devices as recited in claim 62 wherein the virtual network address includes a non-routable IPV4 compliant address.

67. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to route network traffic via the public network from a first device having a public network address to a second device having a different public network address.

68. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to route network traffic from a first device in a private physical network having a private network address to a second device having a public network address.

69. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to route network traffic from a first device in a private physical network having a first private network address to a second device in a different private physical network having a second private network address.

70. One or more processor readable storage media devices as recited in claim 69 wherein the network traffic is routed to the first or second device via a NAT device.

71. One or more processor readable storage media devices as recited in claim 69 wherein the first private network address and the second private network address are identical.

72. One or more processor readable storage media devices as recited in claim 67 wherein the network traffic is routed as encapsulated data packets.

73. One or more processor readable storage media devices as recited in claim 67 wherein the network traffic is routed as encrypted data traffic.

74. One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed, implements the virtual network manager to apply a group policy to the devices that are registered as the members of the virtual network.

75. A virtual network system, comprising: a computing device that includes at least a memory and a processor configured to implement a virtual network manager having a network interface coupled to a virtual network, the virtual network manager including at least one virtual community definition that is defined by a domain name having an associated public network address and a user set of one or more devices that are registered in the virtual network, each device in the virtual network being identified to the other devices by a virtual network address that is associated with the device, the virtual network manager configured to exchange virtual network information with the one or more devices of the user set, the virtual network being accessible by devices in the user set and devices outside of the user set, and the virtual network manager further configured to receive a DNS request from a source device, and return a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device.

76. The system of claim 75 wherein the virtual network manager includes a member register module.

77. The system of claim 75 wherein the virtual network manager includes a member join module.

78. The system of claim 77 wherein the member join module provides a virtual network address to a device that is registered as a member of the network.

79. The system of claim 75 wherein the virtual network manager is further configured to maintain data on an association between at least one virtual network address with at least one device that is registered as a member of the network.

AA/SWA Ex. 1015, p.432 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

80. The system of claim 75 wherein the virtual network manager includes a DNS server for the virtual community network.

81. The system of claim 75 wherein the virtual network manager includes a NAT device detector for devices connecting with the virtual network manager behind a NAT device.

82. The system of claim 75 wherein the virtual network manager includes at least a second virtual community definition.

83. The system of claim 75 wherein the virtual network manager includes a member authenticator.

84. The system of claim 75 wherein the virtual network manager includes a DNS server configured to provide authoritative responses for DNS queries from devices in the virtual community.

85. The system of claim 75 further comprising at least one route director configured to communicate with the one or more devices in the user set.

86. The system of claim 75 wherein each device registered in the network is configured to communicate with the virtual network manager and other devices in the user set via at least one agent.

87. The system of claim 75 wherein the user set includes at least a first device and a second device, and wherein at least one of said first device and said second device is coupled to a first private network and accesses a public network via a NAT device.

88. The system of claim 87 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

89. The system of claim 75 wherein communications between the one or more devices in the user set are encrypted.

90. The system of claim 89 wherein the virtual network manager is configured to provide a shared message to the one or more devices in the user set to establish encrypted communications.

Original

Families

Display in a list (/api/control?client=&familiesSearch=_) INPADOC

This section contains all family relations of this particular document. For more information about the different families, refer to the User Manual (Glossary/Families).

Extended (2) Priority date/claims	Complete (2) Priority date/claims	Main (2) Priority date/claims	Domestic (2) Priority date/claims	Publication number	Application number	Title	Status
2003-03-31 US10403818	2003-03-31 US10403818	2003-03-31 US10403818	2003-03-31	US7949785B2	US10403818	Secure virtual community network system	Granted
				US20040249911A1	US10403818	Secure virtual community network system	Granted

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This Application is related to the following Applications: U.S. Pat. No. 7,139,828 issued Nov. 21, 2006; U.S. patent application Ser. No. 10/161,573, "Creating A Public Identity For An Entity On A Network," filed on Jun. 3, 2002; U.S. patent application Ser. No. 10/233,288, "Communicating With An Entity Inside A Private Network Using An Existing Connection To Initiate Communication," filed on Aug. 30, 2002; U.S. patent application Ser. No. 10/403,829 "Secure Virtual Address Realm," filed on Mar. 31, 2003; and U.S. patent application Ser. No. 10/403,518 "Group Agent," filed on Mar. 31, 2003. All of these related applications are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention is directed to a network services system.

[0004] 2. Description of the Related Art

[0005] Networked data devices provide users with efficient means for communication and collaboration. In recent years, the Internet has played a central role in allowing different types of networked devices to connect and share information across a myriad of networks. As technology advances and more organizations and people rely on the Internet, new challenges are presented for enhancing the ability to communicate. One such challenge is to enable the rapid creation of a secure means that allows local and remote specified entities to communicate and collaborate from any location via a standard Internet connection. For any solution to be widely accepted, it must take into account the realities and limitations currently existing.

[0006] For communication on the Internet, the Internet Protocol (IP) has become the default protocol used by most hosts and to which communication applications are now written. To transmit data from a source to a destination, the Internet Protocol uses an IP address. An IP address is four bytes long and consists of a network number and a host number. When written out, IP version 4 addresses are specified as four numbers separated by dots (e.g. 198.68.70.1). Users and software applications do not always refer to hosts or other resources by their numerical IP address. Instead of using numbers, they use ASCII strings called domain names. The Internet uses a Domain Name System (DNS) to convert a domain name to an IP address.

[0007] The Internet Protocol has been in use for over two decades. It has worked extremely well, as demonstrated by the exponential growth of the Internet. Unfortunately, the Internet is rapidly becoming a victim of its own popularity, it is running out of addresses.

[0008] One popular solution to the depleting address problem is Network Address Translation (NAT). This concept includes predefining a number of network addresses to be private addresses and public addresses. Public addresses are unique addresses that should only be used by one entity having access to the Internet. That is, no two entities on the Internet should have the same public address. Private addresses are not unique and are typically used for entities not having direct access to the Internet. Private addresses are used in private networks. Private addresses can be used by more than one organization or network. NAT assumes that all of the machines on a network will not need to access the Internet at all times. Therefore, there is no

AA/SWA Ex. 1015, p.433 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

need for each machine to have a public address. A local network can function with a small number of one or more public addresses assigned to a NAT device. The remainder of the machines on the network will be assigned private addresses. Since entities on the network have private addresses, the network is considered to be a private network.

[0009] When a particular machine having a private address on the private network attempts to initiate a communication to a machine outside of the private network (e.g. via the Internet), the NAT device will intercept the communication, change the source machine's private address to a public address and set up a table for translation between public addresses and private addresses. The table can contain the destination address, port numbers, sequencing information, byte counts and internal flags for each connection associated with a host address. Inbound packets are compared against entries in the table and permitted through the NAT device only if an appropriate connection exists to validate their passage. One problem with a many NAT implementations is that it only works for communication initiated by a host within the private network to a host on the Internet that has a public IP address. Many NAT implementations will not work if the communication is initiated by a host outside of the private network and is directed to a host with a private address in the private network.

[0010] For most organizations, the security of devices coupled to the Internet is a concern. As a result, not all devices are directly connected to or accessible via the Internet. Rather, many devices are placed in private networks for security concerns (in addition to the address usage issue described above). Many private networks are secured by placing a firewall device between the private network and the Internet.

[0011] Another problem with many current communication schemes is that mobile computing devices can be moved to new and different networks, including private networks. These mobile computing devices may need to be reachable so that a host outside of the private network can initiate communication with the mobile computing device. However, in this case the problem is two-fold. First, there is no means for allowing the host outside of the private network to initiate communication with the mobile computing device. Second, the host outside the private network does not know the address for the mobile computing device or the network that the mobile computing device is currently connected to.

[0012] Thus, there is a need for a system that provides for local and remote entities to communicate and collaborate using the Internet, can work with existing NAT devices and firewalls, and allows for devices to move to different physical networks. To increase the ability of such a system to be accepted by the Internet community, it is desirable for such a system to not require changes to existing applications, allow peer-to-peer applications to communicate directly across the Internet and to not require changes to existing protocols. Each of these issues will be discussed below.

[0013] Large amounts of resources have been used to purchase and deploy existing applications currently running on the millions of computing devices. Organizations and individuals are not likely to want to adopt new communications solutions that require them to absorb the additional cost of replacing all of their applications.

[0014] To provide efficient and secure communication, it is desirable for devices to have the ability to allow their IP based applications to communicate directly with each other. By allowing peer-to-peer applications to communicate directly across the Internet, security is enhanced since the recipient is specifically identified and communication is passed directly between the applications on two or more respective machines.

[0015] Most machines on the Internet use the TCP/IP (Transmission Control Protocol/Internet Protocol) reference model to send data to other machines on the Internet. The TCP/IP reference model includes four layers: the physical and data link layer, the network layer, the transport layer, and the application layer. The physical layer portion of the physical and data link layer is concerned with transmitting raw bits over a communication channel. The data link portion of the Physical and Data Link layer takes the raw transmission facility and transforms it into a line that appears to be relatively free of transmission errors. It accomplishes this task by having the sender break the input data up into frames, transmit the frames and process the acknowledgment frames sent back by the receiver.

[0016] The network layer permits a host to inject packets into a network and have them travel independently to the destination. On the Internet, the protocol used for the network layer is the Internet Protocol (IP).

[0017] The transport layer is designed to allow peer entities on the source and destination to carry on a “conversation.” On the Internet, two protocols are used. The first one, the Transmission Control Protocol (TCP), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error to another machine on the Internet. It fragments the incoming byte stream into discrete segments and passes each one to the network layer. At the destination, the receiving TCP process reassembles the received segments into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more segments than it can handle. The second protocol used in the transport layer on the Internet is the User Datagram Protocol (UDP), which does not provide the TCP sequencing or flow control. UDP is typically used for one-shot, client server type requests-reply queries for applications in which prompt delivery is more important than accurate delivery.

[0018] The transport layer is typically thought of as being above the network layer to indicate that the network layer provides a service to the transport layer. Similarly, the transport layer is typically thought of as being below the application layer to indicate that the transport layer provides a service to the application layer.

[0019] The application layer contains the high level protocols, for example, Telnet, File Transfer Protocol (FTP), Electronic Mail-Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP).

[0020] FIG. 1 depicts the basic structure of an IP version 4 packet **10** used at the Network Layer. IP packet **10** consists of header **12** and payload **14**. Payload **14** stores the data received from the Transport Layer in the TCP/IP model. FIG. 2A depicts the format of a header of an IP packet. The header is depicted to include six rows. The first five rows are 32 bits wide. The first five rows of the header comprise a 20 byte fixed portion of the header. The last row of the header provides a variable sized options field **22**. Version field **24** keeps track of which version of the protocol the packet belongs to. The current version used on the Internet is version 4. IHL field **26** describes the length of the header in 32 bit words. Type field **28** indicates the type of service requested. Various combinations of reliability and speed are possible. Length field **30** contains the size of the packet, including both the header and the data. Identification field **32** is needed to allow the destination host to determine which packet the received fragment belongs to. All fragments of a packet contain the same identification value. Next comes three flags, which include an unused bit **33** and then two 1 bit fields **34** and **36**. DF field **34** stands for don=t fragment. It is an order to the routers not to fragment the packet because the destination is incapable of putting the pieces back together again. MF field **36** stands for more fragments. All fragments except for the last one have this bit set. Fragment offset field **38** indicates where in the current segment this fragment belongs. Time to Live field **40** is used to limit packet lifetime. It is supposed to count time in seconds, allowing a maximum life time of 255 seconds. In practice, it may count hops (or hops and seconds). The time is decremented on each hop by a router. When the time to live hits 0, the packet is discarded and a warning is sent back to the source using an Internet Control Messaging Protocol (ICMP) packet. This feature prevents packets from wandering around forever. Protocol Field **42** indicates which transport layer type is to receive the segment. TCP is one possibility, UDP is another. Checksum field **44** verifies the header. One method for implementing a checksum is to add up all 16 bit half words constituting the header and take the ones compliment of the result. Note that the checksum must be recomputed at each hop because the Time to Live field **40** changes or the content of the options field changes. Source field **46** indicates the IP address for the source of the packet and destination field **48** indicates the IP address for the destination of the packet. Options field **22** is a variable length field designed to hold other information. Currently, options used on the Internet indicate security, suggested routing path, previous routing path and time.

[0021] UDP is an alternative to TCP. FIG. 2B depicts the structure of a packet that uses UDP. Like the TCP, UDP uses the Internet Protocol to actually send a data unit from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP does not provide sequencing of the packets that the data arrives in. Hence, application

AA/SWA Ex. 1015, p.434 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

programs using UDP must ensure that the entire message has arrived and is in the right order. As shown in FIG. 2B, the packet includes an IP header **12***a* and IP payload **14***a*. The payload **14***a* comprises the UDP header **50** and UDP data **60**. UDP header **50** consists of a 16 bit source port identifier, a 16 bit destination port identifier, a length field and checksum field. In FIG. 2B, the Destination Port has a meaning within the context of a particular Internet destination address, and the Length field is the length in octets of this user datagram, including its header and the data. The checksum is the 16-bit one's complement of the sum of consecutive two octaves of a pseudo header of information from the IP header, the UDP header, and the data (padded with zero octets at the end, if necessary, to make a multiple of two octets).

[0022] In addition to using the existing Internet infrastructure, another issue in allowing public-to-private, or private-to-private, communications lies in the addressing of the devices. Where a system is coupled to the public Internet with an IP address, communication packets can be routed directly to the machine. However, many devices couple to the Internet via service providers which provide them with a dynamic IP address. Thus, those wishing to communicate with this type of user must know the constantly changing address of the user in order to communicate with them. Still other hosts may be coupled to networks that use technologies other than IP.

[0023] One solution currently in use that provides for local and remote specified entities to communicate and collaborate using the Internet is the Virtual Private Network ("VPN"). The VPN uses additional network software layers to increase security between users in the public realm and those in private realms. For example, some VPNs encrypt packets using IPsec (or other protocols). The encrypted packets are then encapsulated within a standard packet and transmitted across the Internet to the destination. At the destination, the encrypted packet is decrypted. While the existing VPN provides remote users with secure access to a network, via the Internet, many existing VPNs have various shortcomings that prevent them from satisfying the needs of many users. For example, many VPNs do not provide for peer-to-peer communication with IPsec (or other security measures), do not work though NAT devices in all cases, are difficult to set up and maintain, do not provide for full mobility of entities communicating on the VPN, and do not always provide for communication with entities in the various private network configurations discussed herein.

[0024] One method of overcoming the mobility problem includes the use of Dynamic DNS. More information about Dynamic DNS can be found in RFC 2136 incorporated herein by reference.

[0025] Dynamic DNS is illustrated in FIG. 3. FIG. 3 shows a first computer or device B having a host name of B.COb.com having a dynamic or static private IP address IPb and a second computer or device A having a host name of A.COa.com and having a dynamic or static private IP address IPa. Devices B and A are coupled to the Internet **506** via firewall devices **302**, **304** incorporating NAT. The addresses of B and A, as seen by devices on the Internet, are public IP addresses GIPb and GIPa, respectively. Also shown is device D, having a publicly address IPd and a host name of d.COd.com.

[0026] Also shown is a Dynamic DNS server, DDNS, residing on the Internet. In essence, the DDNS server is a DNS server supporting the dynamic DNS protocol of RFC 2136, and in this example is an authoritative name server containing records for B, A and D. The DDNS server will update it's records of B, A and D in real time, so that if or when D's address IPd changes, any query by other devices (B, A, for example) based on D's host name, will result in the response being the correct IP-IPd. Any DNS records for devices B and A will always reflect the public IP addresses (GIPa and GIPb) of the firewall/NAT devices.

[0027] Unfortunately, DDNS technology is complex and difficult to implement securely—two factors that have dramatically slowed the rate of deployment of Dynamic DNS. As a result, VPNs have not been able to adopt DDNS to solve all of the problems discussed herein.

[0028] Hence, a system is desired that allows local and remote entities to communicate and collaborate from any location via a standard Internet connection and which solves the problems discussed above.

SUMMARY OF THE INVENTION

[0029] A system is disclosed that allows local and remote entities to communicate and collaborate from various locations. In one embodiment, the system makes use of a virtual subnet with a virtual address realm. The virtual address realm allows two or more users to communicate securely via at least one public network, whether the users are both coupled directly to the public network, both coupled directly to separate private networks or whether one is in a public network and one is in a private network. The virtual address realm uses virtual addresses to identify the devices on the virtual subnet. Although the devices are in different physical subnets, from the point of view of the applications the devices of the virtual subnet appear to be in one local subnet.

[0030] In one embodiment, the virtual address realm comprises a virtual address realm definition including at least a set of users. Each user accessing the virtual address realm may have at least one virtual address in the virtual address realm and at least one physical address.

[0031] Another embodiment of the present invention comprises a virtual community network for transmitting communications via at least one physical network. The virtual community network comprises a virtual address realm including a logical name assignment, a set of users capable of communicating in the virtual address realm, and a secure communication channel. In a further aspect, the virtual community network logical name is a domain name, and the domain name may be a fully qualified domain name or a virtual domain name. In another aspect, the set of users includes at least a first user coupled to a first private physical network and a second user coupled to a second private physical network, and the first private physical network and the second private physical network may have at least one common private physical subnet address. The physical addresses may be dynamic or static.

[0032] Yet another embodiment of the invention is a method comprising the steps of: defining a virtual address realm overlying a public address realm, the virtual address realm including at least a user set and a logical name for said user set; and routing communications between users in the user set by means of virtual address realm addresses. In a further aspect, this method includes the step of registering users in the user set as members of the virtual address realm. Further, the method may include the step of assigning each registered user a unique virtual address in the virtual address realm. The method may further include the steps of encrypting communications between devices in the realm, and/or applying at least one address realm group policy.

[0033] A further embodiment of the invention is a method for providing secure communications between two devices. The method comprises the steps of: providing a virtual realm identifier; defining a set of users for the virtual realm; registering users in the realm; assigning virtual addresses; and routing information between users in said virtual address realm.

[0034] A still further embodiment of the invention comprises one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices. In this embodiment, said processor readable code is for programming one or more processors to perform a method comprising the steps of: providing a virtual address realm configuration including a user set and a domain name for said user set; and routing communications between users in said virtual address realm.

[0035] Another embodiment of the invention comprises a method for providing a secure virtual network. The method may include the steps of: providing a virtual network manager coupled to a public network; defining a member set of users entitled to communicate in the virtual network; registering members with the manager; assigning members a virtual address; and routing network traffic between the members in the virtual community.

AA/SWA Ex. 1015, p.435 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

[0036] An additional further embodiment of the invention may comprise one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices. The processor readable code may be for programming one or more processors to perform a method comprising the steps of: managing a virtual community network realm; defining a member set of users entitled to communicate in the virtual community; registering users with the virtual community; assigning each user a virtual address; and routing network traffic between the users in the virtual community.

[0037] Another embodiment of the invention is a virtual community network system. The system includes a virtual network manager including at least one virtual community definition comprising at least a domain name and a user set; and at least one route director capable of communicating with users in the user set.

[0038] In a further aspect, the virtual community network includes a communication agent installed on a device. The agent may comprise a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address.

[0039] For some devices, additional software or hardware cannot be installed on a member device or it is not desirable to install such additional software or hardware on the device. For such devices, a Group Agent can be used. The Group Agent acts as a proxy for one or more members of a virtual community without requiring installation of member agent software on the client devices.

[0040] One embodiment of a system that uses a Group Agent includes communicating with a first client and acting as an intermediary between the first client and members in a first virtual address realm so that the first client can communicate in the first virtual address realm. Note that in this embodiment the first client is not configured to communicate in the first virtual address realm. For example, no software is installed on the client to add drivers, layers or interfaces specific to the first virtual address realm.

[0041] Another embodiment of a system using a Group Agent includes communicating messages with a first client and communicating the messages with members in a virtual address realm on behalf of the first client. While communicating with the first client, the messages do not use virtual addresses. During the communication process, the messages are transformed so that the messages include virtual addresses when communicating with members in the virtual address realm and the messages do not include virtual addresses when communicating with the first client.

[0042] In one implementation, the first entity resides in a first physical address realm and the second entity resides in a second physical address realm, where the first physical address realm overlaps with the second physical address realm. For example, consider the situation where the first physical address realm is a first private network using a first set of private addresses and the second physical address realm is a second private network using a second set of private addresses, where there are private addresses that exist in both the first set of private addresses and the second set of private addresses.

[0043] The present invention can be accomplished using hardware, software, or a combination of both hardware and software. The software used for the present invention is stored on one or more processor readable storage media including hard disk drives, CD-ROMs, DVDs, optical disks, floppy disks, tape drives, RAM, ROM or other suitable storage devices. In alternative embodiments, some or all of the software can be replaced by dedicated hardware including custom integrated circuits, gate arrays, FPGAs, PLDs, and special purpose computers. In one embodiment, software implementing the present invention is used to program one or more processors. The processors can be in communication with one or more storage devices, peripherals and/or one or more communication interfaces.

[0044] These and other objects and advantages of the present invention will appear more clearly from the following description in which the preferred embodiment of the invention has been set forth in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0045] The invention will be described with respect to the particular embodiments thereof. Other objects, features, and advantages of the invention will become apparent with reference to the specification and drawings in which:

[0046] FIG. 1 depicts an IP packet.

[0047] FIG. 2A depicts the format of a header of an IP packet.

[0048] FIG. 2B depicts the format of a UDP packet.

[0049] FIG. 3 depicts a print-out implementation of a dynamic routing system.

[0050] FIG. 4 depicts a block diagram of an implementation of the system of the present invention.

[0051] FIG. 5A is a structural network block diagram illustrating elements used in the system of the present invention.

[0052] FIG. 5B is a logical block diagram depicting communication types in an implementation of the system of the present invention

[0053] FIG. 6A depicts a packet structure for a communication packet in accordance with the present invention.

[0054] FIG. 6B is a table depicting the shim configuration of the packet in FIG. 6A.

[0055] FIG. 7 is a flow chart describing the overall process for communicating.

[0056] FIG. 8 is a block diagram illustrating the structure of the Member Agent application in the system of the present invention.

[0057] FIG. 9 is a flowchart illustrating the steps which occur in the creation of a virtual community.

[0058] FIG. 10 is a flowchart illustrating the process of configuring a virtual community.

[0059] FIG. 11 depicts an HTTP wrapper structure.

[0060] FIG. 12A is a flow diagram depicting a user registration process of the present invention.

[0061] FIG. 12B is a table illustrating the structure of the registration file information structure.

[0062] FIG. 13 is a flowchart depicting a member join process in accordance with the present invention.

[0063] FIG. 14 is a flowchart depicting a member leave request in accordance with the present invention.

[0064] FIG. 15 is a flow diagram depicting DNS request for a member in the virtual community in accordance with the present invention.

[0065] FIG. 16A depicts the commonly used IKE phase one aggressive mode exchange.

[0066] FIG. 16B depicts the IKE phase one aggressive mode exchange used in accordance with the present invention.

[0067] FIG. 17 depicts a packet structure of the virtual IKE phase 1 packet.

AA/SWA Ex. 1015, p.436 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

[0068] FIG. 18 depicts the IKE ticket payload data structure.

[0069] FIG. 19 is a representation of a system ping sequence in accordance with the present invention.

[0070] FIG. 20 is a flow diagram depicting a query request in the system of the present invention.

[0071] FIG. 21 depicts a flow structure for addressing and routing conducted by a Route director.

[0072] FIG. 22 is a block diagram depicting one embodiment of various components of the present invention utilizing a Group Agent.

[0073] FIG. 23 is a flow chart describing one embodiment of the process for Group Agent initialization.

[0074] FIG. 24 is a flow chart describing one embodiment of a process for initiating communication with a member that is using a Group Agent.

[0075] FIG. 25 is a flow chart describing one embodiment of a process for communicating using a Group Agent.

[0076] FIG. 26 is a flow chart describing one embodiment of a process for initiating communication by a member that is using a Group Agent.

DETAILED DESCRIPTION

[0077] One embodiment of the present invention provides for a secure Virtual Community Network or "VCN." In essence, a VCN is a private dynamic network which acts as a private LAN for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. Thus, the invention provides a separate private virtual address realm, seen to each user as a private network while seamlessly crossing public and private network boundaries.

[0078] A basic overview of the system is shown in FIG. 4. FIG. 4 shows a computer or device B (host name—b.COb.com) in a first private domain and computer or device A (host name—a.COa.com) in a second private domain, both of which are coupled to the Internet by firewall devices **402**, **404**. The firewall devices are configured to implement Network Address Translation (NAT). A and B have dynamic or static private IP addresses. Computer or device X is coupled directly to the public Internet and has a public IP address.

[0079] In the present invention, a virtual community network (VCN) X.VCN is formed. Machines A, B and X can join the VCN, leave the VCN, or allow other machines in the VCN to communicate with them. More than simply a virtual private network (VPN), all members of the VCN are accessible as if they were part of a physical local network. The application running on the members of the VCN can accomplish what they would be able to accomplish if they were on the same physical routed network (e.g. all in the same private network). Membership in the VCN is controlled by an administrator via an administrative interface. In general, the administrator defines certain aspects of the VCN and then invites members into the VCN by specifying the domain name for each member. Members then register themselves with a VCN Manager, and notify the Manager via join and leave requests when they are available to participate in the community. Once registered and joined, members can communicate with other members as though connected via a local LAN.

[0080] As shown in FIG. 4, A, B and X may all make direct connections to each other through communications within the virtual domain. In FIG. 4, dashed lines represent direct communication paths seen to applications running on A, B and X, all "seeing" the virtual addresses of each other and communicating with each other using the application's IP interface.

[0081] A hardware architecture for the machines, server or other devices used to implement the present invention should be well understood to one of average skill in the art. Suitable hardware includes one or more processors, a memory, a mass storage device, a portable storage device, a first network interface, a second network interface and I/O devices, in communication with each other. The choice of processor is not critical as long as a suitable processor with sufficient speed is chosen. The memory can be any conventional computer memory. The mass storage device can include a hard drive, CD-ROM or any other mass storage device. The portable storage can include a floppy disk drive or other portable storage device. If the computer is acting as a router, it includes two or more network interfaces. In other embodiments, the computer may include only one network interface. The network interface can include a network card for connecting to an Ethernet or other type of LAN. In addition, one or more of the network interfaces can include or be connected to a firewall. For a gateway, one of the network interfaces will typically be connected to the Internet and the other network interface will typically be connected to a LAN. However, a gateway can exist physically inside a network. I/O devices can include one or more of the following: keyboard, mouse, monitor, display, printer etc. Software used to perform the methods of the present invention are likely to be stored in mass storage (or any form of non-volatile memory), a portable storage media (e.g. floppy disk or tape) and/or, at some point, in memory. The above described hardware architecture is just one suitable example depicted in a generalized and simplified form. The present invention could include dedicated hardware, a dedicated router with software to implement the invention or other software and/or hardware architectures that are suitable.

[0082] A more detailed overview of one embodiment of the present invention is depicted in FIGS. 5A and 5B. FIG. 5A illustrates various embodiments of devices coupled to public and private networks in a manner which allows use of the present invention, and is a representation of a physical connection of such devices. FIG. 5B illustrates a logical representation of elements used to create a VCN and of the various formats of communication traffic between those elements shown in FIG. 5A.

[0083] Specifically, FIGS. 5A and 5B illustrate various user machines M_n coupled to the Internet **506**, as well as other devices, described below, which implement a virtual community in accordance with the present invention. Devices M_n can be personal computers, servers or other computing devices (mobile or non-mobile). Each machine may have different communication connectivity with the Internet.

[0084] In general, an exemplary system for implementing a VCN in accordance with the invention comprises a VCN Manager **510**, a Network Route Director **520** and/or Private Route Director **530**, and a number of Member Agents **565**. Communication between systems in various protocols is illustrated by dashed lines (UDP) and solid lines (TCP). The VCN manager and Network Route Director are shown in FIG. 5A as being coupled directly to Internet **506**.

[0085] User devices M_A and M_E are connected to the Internet and have public IP addresses. These addresses may be dynamic or static. If static, M_A and M_E can easily communicate with each other in a manner well known in the art by simply addressing IP packets directly to each other. If the addresses are dynamic, then M_A and M_E require some means of knowing when the IP address of the other changes in order to communicate. As described below, the VCN system provides such a means.

[0086] Device M_B is in a private domain (e.g. private network)) **540** and connected to a NAT Device **515** to access the Internet **506** by a private network path **540***a*. Device M_B may use have a dynamic or static IP address specific to the private domain **540**. Generally, such addresses are part of the private received IP classes which are not routable via the Internet. For example, 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 are network addresses classified for private networks. Firewall/NATdevice **515** translates Machine M_B's private IP address to a routable public IP address. NAT device **515** may include other security functions as well. M_B communicates with other non-VCN devices on the Internet via the NAT device **515**, and with other members of the VCN via Private Route Director (PRD) **530**, which is coupled to the private network path **540***a* and is a member of the private network **540**. Device M_X is also shown as connected to and a member of the private domain **540** but has a static, routable public IP addresses. As such it may communicate with devices coupled to Internet **506** in a different manner, as illustrated in FIG. 5B.

AA/SWA Ex. 1015, p.437 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

[0087] Devices M_C and M_D are part of a second private domain (e.g. private network) **550** coupled to a second private network path **550***a*. Again, these machines have static or dynamic private IP addresses and are coupled to the Internet via a firewall/NAT device **517**, which is itself coupled to network path **550***a*.

[0088] The VCN Manager **510** is a central server or server cluster providing management services, connection services and security services for the VCN. Each Member Agent **565** includes client agent software (or, in some embodiments, hardware) that runs on end machines and provides virtual network services. It enables the machine to be reached from public and private networks, and implements the security aspects of the system. In FIG. 5B, machines M_A, M_B, M_C, M_D, M_E and M_X all include Member Agents and, therefore, can be members of a particular VCN.

[0089] The Network Route Director (NRD) **520** is a stand-alone unit that runs on the public side of the Internet enabling Member Agents and Group Agents (discussed below) to be reached inside one or more private networks from the public network. Private Route Director ("PRD") **530** is an element that runs inside a private network enabling access to machines inside the private network from machines outside the private network. It can run as a service on a platform offering other services such as a Windows Server.

[0090] Generally, VCNs are defined and managed by the VCN Manager **510**. Clients utilize Member Agents or Group Agents to access other client machines (M_n), in private or public realms. The NRD or PRD routes communications to Member Agents.

[0091] As described herein, three forms of communication are used in creating and implementing the VCN. TCP is used in the registration and joining processes; encapsulated UDP packets are used between elements in establishing communication between joined devices and for management traffic, and Encrypted UDP packets are used for agent-to-agent communications.

[0092] FIG. 5B shows exemplary traffic between elements of the VCN. A first type of traffic is TCP traffic. TCP traffic is used between member agents to establish membership in the VCN (the registration process), and make the VCN manager aware they are available to communicate with other members of the VCN (the join process). In FIG. 5B, this is represented by solid lines **513***b*, **511***b*, **523***b* and **543***b*. TCP is also used: by the PRD **530** to establish communications with the VCN (lines **527***b*, **527***d*); and by the member agent of device M_B to communicate with the PRD **530** (line **533***b*). TCP may also be used by devices M_C and M_D on private network **550** to communicate with each other.

[0093] Encapsulated UDP traffic is used by elements of the VCN once membership has been established and the elements are joined in the VCN for management and administrative communications. This is represented in FIG. 5B by lines **511***a*, **513***a*, **523***a*, **527***a*, **527***c*, **523***c*, **527***e*, **521**, **543***a*, **541**, and **519**. Encrypted UDP communications are used between devices, shown in FIG. 5B between device M_X and M_A at **525** and device M_B and M_C at **537**.

[0094] In one embodiment, secure connections are built dynamically using IPsec tunnels based on a virtual IP space that can traverse from private networks, across the Internet and into other private networks. Strong authentication and the establishment of IPsec policies at the time members join the community offers privacy and security to the members of the virtual community. This facilitates the introduction of a variety of policy-based network services with centralized management such as Virtual Private Networks for intranets and extranets, IP-telephony domains, and IP-based PDA communities.

Communication Protocol

[0095] In the present invention, an encapsulation routing protocol allows packets to traverse addressing boundaries and identifies routing endpoints by unique DNS domain names. It employs an address virtualization scheme that accomplishes backwards compatibility with IPv4 applications. With certain optional exceptions, UDP encapsulation is used between elements of the Virtual Community.

[0096] One example of an encapsulated packet **600** is depicted in FIG. 6A. It includes a 20 octet IP header **602**, an 8 octet UDP header **604**, a 20 octet system shim **606**, and a variable size virtual IP packet **608**. A virtual IP packet has the same format as a standard IP packet.

[0097] Members of a VCN communicate to other members of that VCN by means of virtual IP Packets **608**. Virtual IP addressing is used to establish unique connection identities for community connected devices. IPsec can (optionally) be applied to the Virtual IP Packet for end-to-end security. Virtual IP addresses are used to identify members in the community in the virtual packet and are not directly routable. Rather, they are unique identifiers of a given connection to the upper layer application. In one embodiment, virtual IP addresses are in IPV4 format.

[0098] In general, the UDP header is set for a default port. System shim **606** carries enough addressing information to allow the Route Directors to forward the tunneled packet through the various address realms on its way to the destination. Such a routing methodology is often referred to as source routing.

[0099] In order to route packets to a peer in a different addressing realm, the protocol stack knows the address of the appropriate Route Director that serves the peer's realm, the private address of the peer or a NAT address. The Member Agent obtains the information by using the VCN Manager as a DNS authority for DNS lookup operations as described below (FIGS. 13 and 21). The DNS response from the VCN Manager will include the above-identified information in an optional text field of the response to the Member Agent.

[0100] TCP/IP connections require IP addresses to be used as connection identifiers at the user level. If an application wishes to make a connection to "m3.abcdef.com" and another to "m4.abcdef.com", it resolves both DNS identifiers into IPv4 addresses. The system cannot assign the private IP addresses of the members to be unique connection identifiers, because two members might have the same private address in different private address realms.

[0101] Assigning a virtual address to each peer designated by a DNS string solves the problem of ambiguous endpoints. These virtual addresses may be any legal IPv4 addresses, but conflicts will occur if the same addresses are used to directly designate a peer in an IPv4 network application. For instance, if 10.0.0.10 is used as a virtual address, and is also used on a member's network as the mail server, packets that are ordinarily destined to the mail server may be redirected to a random peer. In general, when choosing virtual addresses it is best to choose addresses that will not be routable to the member. Hence, each member is assigned a virtual IP address unique in the context of the virtual community and that will not conflict with any local addresses on its LAN or any public IP addresses on the Internet.

[0102] By having each member of a VCN use a virtual address, a virtual address realm is created. The virtual address realm is the set of addresses that can be used to identify and send communications to other members of the VCN. The virtual address realm is different from a physical address realm because the physical address realm is actually used to route on a physical network. The members of a VCN will all be in the virtual address ream of that VCN, but may be in different physical address realms. For example, looking at FIGS. 5A and 5B, M_B and M_C are in different physical address realms (e.g. **540** and **550**); however, they are both in the virtual address realm of the VCN. Another example can be seen with FIG. 4, where A and B are in different physical address realms (Cob.com and Coa.com); however, they are both in the same virtual address realm. Applications on members of a VCN will see the VCN as the local subnet; therefore, the VCN can be thought of as a virtual subnet. Each member of the VCN will appear to the application as an entity connected to the local subnet.

[0103] Route Directors **530** and **520** facilitate routing UDP encapsulated traffic to private address domains **540**, **550**. In general, Route Directors either have public IP addresses or addresses that are statically remapped to a public IP address. The static translation of a Route Director's IP must leave the port in the UDP header unchanged to allow the UDP encapsulated destination port number to be directly used by public members, by other Route Directors, and by private members. Route Directors **520**, **530** and VCN Manager **510** may be configured to use a non-default UDP encapsulation port. In

AA/SWA Ex. 1015, p.438 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

one embodiment, all outgoing messages are sent to this port on the next destination node and all incoming messages are read from this port. As discussed below, information in a "join" packet tells Member Agents the UDP encapsulation port to use in communications to Route Directors, network managers, and other members of the community.

[0104] System Shim **606** (see FIG. 6A) has a format given by way of example in FIG. 6B. Protocol Version information, data type, header option flags, and Router Information are potentially stored in the Shim. (The abbreviation "gIP" stands for "global" or public IP address, indicating an Internet routable IP address). The Data Type field indicates the meaning of the optional data that may follow the Shim. This may include a Virtual IP Packet **608**, a ping to a Route Director, a request for a Network Route Director virtual address, a Route Director response with a virtual address, a member leaving and releasing a virtual address, and a member-to-Route Director packet. The shim also includes the public IP address for the source machine's Route Director, the public IP address for the destination machine's Route Director, the private IP address for the source machine and the private IP address for the destination machine. In the case where the source or destination use a public IP address, then the shim will not need to include the private addresses of the source/destination or a route director.

[0105] The system can optionally use TCP encapsulation between a member and a Route Director. If the VCN Manager determines that a Member Agent (e.g., Agent software on a member machine) and a Route Director are both able to support a TCP connection, then it may instruct the member to initiate a TCP connection with the Route Director. TCP port **80** may be used as the destination port for all TCP encapsulated messages to the Route Director, and TCP port **20202** may be used as the source port for all TCP encapsulated messages from a private member to the Route Director.

[0106] As noted above, Network Route Directors (NRDs) **520** facilitate routing traffic into and out of private address domains without requiring reconfiguration of a firewall **517** protecting the domain **550**. As in UDP encapsulation, a special field in the system join packet (explained below) tells the Member Agent which TCP encapsulation port to use as the source port. The NRD will then re-encapsulate virtual-traffic in UDP-encapsulation before passing it on to other elements of the virtual network.

[0107] Note that more than one user can use the same device, with each such user having different virtual addresses in the same or different address realms. Additionally, regardless of the number of users, one device can be in multiple virtual address realms. In some embodiments, a user can have multiple identities, each in a different address realm.

[0108] FIG. 7 is a flow chart describing the overall process for communicating between members of a VCN. Any member of a VCN can communicate with any other member of a VCN regardless of whether either of the members are behind a firewall, behind a NAT device, directly accessible via the public Internet, in a private network, etc. From the point of view of an application on a member device, all the other members appear to be on the same LAN. Thus all applications running on a member's device will think that all other members of the VCN are on the same LAN and in the same address realm (e.g. the virtual address realm of the VCN).

[0109] In step **650** of FIG. 7, the Agent for the potential member joins the VCN and receives a virtual IP address. In order to establish or participate in communication within the VCN, a device must register with and join the VCN, thereby becoming a member of the VCN. The Agent will send a message to VCN Manager **510** and receive a virtual IP address back. The virtual IP address received is used to identify the member in the VCN. More details of step **650** as well as other portions of FIG. 7 will be discussed below. Note that there is a dotted line between step **650** and step **652**. This dotted line signifies that a lot of time can pass between step **650** and step **652**. Additionally, after step **650** is performed, it does not need to be repeated.

[0110] In step **652** of FIG. 7, an application on the source machine (the member initiating communication) intends to send a message to an application on the destination machine (another member of the VCN). Examples of applications that can communicate on the VCN include instant messaging, email, FTP, browsers, data transfer programs, and other applications that can communicate. Consider an example when application on device M_A intends to initiate communication with an application on device M_B. Thus, M_A is the source device and M_B is the destination device. In step **654**, the application on M_A will initiate a DNS request using the domain name for M_B. This DNS request is sent to VCN Manager **510**. In step **656**, VCN Manager **510** returns the public address of the Route Director for the destination, the private address for the destination device and a virtual IP address for the destination device. In the example described above, step **656** includes returning the public IP address for private Route Director **530**, the private address for M_B and a virtual IP address for M_B. If the destination machine has a public IP address (and, thus, does not use a routing director) then step **656** will only include returning the public IP address for the destination. If the destination machine is in a private network that uses a Network Route Director (e.g., NRD **520**), then step **656** will return the public IP address for the Network Route Director.

[0111] In step **658**, the Agent for the source device, which received the information in step **656**, will store that received information. This information can be stored in a table, or any other data structure. In step **660**, the Agent for the source device will return the virtual IP address of the destination device to the application on the source device. In step **662**, the application on the source device will initiate the sending of a message/data using the virtual IP address for the destination device. In step **664**, a virtual IP packet will be created. The source IP address for the virtual IP packet will be the virtual IP address for the source device. The destination IP address for the virtual packet will be the virtual IP address for the destination device. The virtual IP packet will be in the same format as a standard IP packet. In step **664**, the newly created virtual IP packet will be subjected to IPsec (or another security means). In some embodiments, IPsec is not used. In step **670**, the virtual IP packet is encapsulated. For example, in one embodiment, the virtual IP packet is encapsulated as described above with respect to FIGS. 6A and 6B. This encapsulation will include shim **630**. As described above, shim **630** will include the public IP addresses for the Route Directors for the source and destination, and the private IP addresses for the source and destination devices. If either the source or destination do not have a Route Director, the shim will not need to include that information. For example, when the source machine is M_A, there is no Route Director for the source. If the source machine was M_C, then the shim, would include the public IP address for Network Route Director **520**. If the source is M_B, the shim would include the public IP address for Private Route Director **530**.

[0112] At this point, the path of the packet will depend on whether the destination is using a Private Route Director **530**, Network Route Director **520** or has a public IP address. If the destination has a public IP address, the process moves to step **678** where the encapsulated packet is forwarded to the destination agent.

[0113] If the destination is in a private network that has a PRD, then in step **672** the encapsulated packet is sent to the NAT device for the destination. For example, the encapsulated packet is sent from M_A to NAT **515**. In step **674**, the encapsulated packet is sent from the NAT device for the LAN that includes the destination to the Route Director for the destination. For example, the encapsulated packet is sent from NAT **515** to private Route Director **530**. In step **676**, the Route Director which received the encapsulated packet will remove the virtual IP packet and the shim from the encapsulation. The Route Director will read the shim to learn the local IP address to send the packet to. The shim and virtual IP address will then be re-encapsulated into a new packet with the original virtual packet. The new outer packet includes a destination IP address equal to the private IP address of the destination device. The encapsulated packet received in step **674** will include a source IP address equal to the public IP address for M_A (or the source's Route Director) and a destination IP address equal to the public IP address for the Route Director of the destination (e.g., PRD **530**). In step **678**, the new encapsulated packet will be sent from the Route Director to the Agent for the destination device.

[0114] If the destination agent is in a private network and is using a Network Route Director, then following encapsulation the encapsulated packet is sent to the Network Route Director for the destination agent in step **673**. At step **675**, the NRD will remove the virtual IP Packet and shim and re-encapsulate them in a UDP packet for transmission through a NAT device to the destination via a persistent UDP connection between the NRD and the destination. At step **677**, the encapsulated packet is forwarded to the NAT device (via the persistent UDP connection) behind which the destination Agent resides, which will perform its own routing of the encapsulated packet to the destination Agent in step **678**.

AA/SWA Ex. 1015, p.439 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

[0115] In step **680**, the Agent will remove the shim and the virtual IP packet from the encapsulation. The virtual IP packet will be removed from IPsec (e.g. decrypted). In step **682**, the information from the shim will be stored by the Agent. In step **684**, the contents of the virtual packet will be presented to the application on the destination device. That is, the application on the destination device will receive the contents of the data payload, or at least a portion of the data payload

[0116] When the destination wishes to respond to the source or the source wishes to send additional information, the process of FIG. 7 can be repeated. However, when repeating the process of FIG. 7 between two machines where communication is already established, the steps of performing the DNS request do not need to be performed again. That is, when the destination wishes to respond, the destination will perform the steps in FIG. 7 starting at step **662**. The Agent for the destination device will already know all the information to put in the shim. Additionally, when the source device wishes to send additional information to the destination device, the source device can start FIG. 7 at step **662**. In some embodiments, however, the steps of performing the DNS request will be performed again.

Member Agent

[0117] As noted above, devices in the VCN utilize a member agent installed on the device to communicate. One unique aspect of the system of the present invention is the integration of the agent software in a typical device.

[0118] FIG. 8 illustrates the functional flow diagram of an installed agent on a device such as a computer, server or other device. Region **810** illustrates the "user space," and region **820** represents the kernel area of the components interacting with the host device.

[0119] Applications **830** interact directly with an IP stack **835** which is built on a deterministic network extender or DNE **850**. The deterministic network extender is provided by Deterministic Networks, Inc. The network extender allows one to implement any driver level functions such as IPsec, browsers, traffic redirectors, and the like, through a series of plug-ins. As shown in FIG. 8, a number of plug-ins, including a DNS plug-in **852**, an IPsec plug-in **854**, a virtual adapter manager **856** and a domain name router **858** (see U.S. Pat. No. 6,119,171, incorporated herein by reference) interact with the deterministic network extender **850**. The DNS plug-in processes DNS queries by applications via the stack. The virtual adapter manager allows for additional adapters to co-exist in the same device.

[0120] The DNE is an NDIS compliant module (in Windows environments) which appears as a network device spire to the protocol stack **835**. The DNE supports the TCP/IP and UDP protocols and various adaptor types. In essence, this forms a virtual network adaptor in device installations. This means that various configurations for each virtual community can be provided for each DNE. This provides the advantage that a number of members or users can utilize the same device, with the device installing a different virtual adaptor using plug-ins for the deterministic network enhancer and each user does not need to reconfigure the network settings of the machine to join each community. Each plug-in is constructed in accordance with standards promulgated by the DNE provider.

[0121] As shown in FIG. 8, user applications interact directly with the IP stack of the virtual adapter. Each adapter provides its own stack to the device's applications. To the applications, each stack appears separate, and no separate routing of the application is required. For example, the IKE user application **825** can interact with the domain name plug-in, the IPsec plug-in, the virtual area management communicator **856**, and the security policy manager **860**. The Adapter Manager **856** allows parallel stacks for each VCN to be implemented and used on each machine. This means a user and device can belong to several VCNs without needing to re-configure IP settings to access each VCN.

VCN Definition

[0122] FIG. 9 shows the steps which occur at the VCN Manager to define and establish a virtual community. At step **902**, an administrator sets up a virtual community by providing information to the VCN Manager via a user interface (not shown). It will be understood that the user interface and the method of providing information to the VCN Manager is not critical to the system of the present invention. One particularly advantageous interface is implemented in a World Wide Web browser. The interface may be implemented using HTML, XML, Java Applets, Java Server, Active Server Pager or any of a number of well-known Web technologies. The particular information required to set up the community network is illustrated in FIG. 10. Next, at step **904**, users who are designated by the administrator as being allowed access to the virtual community defined in step **902** are notified by any number of appropriate means. In one implementation, the users are notified by e-mail, although other forms of notification, such as verbal or personal notification, may be used. The e-mail may contain an invitation to join the community, community authentication information, a link to a location to download the Member Agent, and/or a link to the Group Agent. Next, at step **906**, using information contained in the e-mail, users register with the VCN Manager. Registration in this context means registering a machine using a Member Agent or a Group Agent with the VCN Manager. Users may be required to install the Member Agent software. The link in the notification e-mail may provide the user with a location for downloading the Member Agent software as well as instructions for installing the software. Other information, such as system password information, is provided in the e-mail. Finally, at step **908**, management of the community is handled by the VCN Manager. This includes monitoring which registered users have joined and left the system, answering DNS requests, and applying security policies, as described herein. This may include notifying new users and registering those users as the definition of the VCN changes.

[0123] FIG. 10 is a flowchart illustrating the process of setting up a virtual community which is performed by an Administrator. Initially, the Administrator sets up a virtual domain name and address domain at step **1002**. This information is used by the VCN Manager and Route Directors to allow members to communicate. Next, users are defined at step **1004**. In one embodiment, the users are defined by providing the domain names of each of the users who will be invited to participate in the VCN. At step **1006**, default passwords are set. This is the password a user first uses to access the system. The user may be forced to change the password for security reasons at a later date. Finally, at step **1008**, polices may be defined at the domain level, the user level, or for individual machines in the domain. Policies are used to allow or deny access to individual machines, services, or other users.

Member Registration

[0124] The registration process is the first step that a user and machine go through with the VCN Manager before becoming a member of a virtual community. There are two phases to member registration: a registration request and a registration file request. Registration happens outside of the IPsec tunnels because at registration time no IPsec tunnel exists for the user registering.

[0125] In one implementation, all traffic between Member Agents and the VCN Manager (with the exception of Registration and Join function traffic is encapsulated using UDP encapsulation, represented by lines **511***a*, **513***a*, **523***a*, **519**, **521**, **527***a*, **527***c*, **537**, **523***c*, **527***e*, **541**, **543***a*, **533***a* of FIG. 5B). This encapsulated traffic will carry management traffic between the members and the VCN Manager. A service port is reserved at the VCN Manager in the virtual network for the establishment of a TCP connection between a member and the VCN Manager. A member that joins a VCN is informed of the service port as part of the join protocol. A DNS port is also open on the virtual side of the VCN Manager. In one embodiment, the VCN Manager virtual ports are TCP Port **9001** and DNS UDP Port **53**. The packets used for the initial Registration and the subsequent Join operations use TCP port **80** outside the virtual network. This is represented in FIG. 5 by the solid lines **513***b*, **511***b*, **523***b* and **543***b*.

[0126] VCN system protocol packets that are sent outside the system tunneling are HTTP wrapped and sent to the VCN Manager on TCP port **80** to facilitate NAT traversal. More information about NAT traversal will be provided below. Each packet includes a header and payload. For compatibility with firewalls, the HTTP wrapper makes the packet a SOAP-compatible XML document. Including a binary data portion after XML is consistent with Direct Internet Message Encapsulation (DIME), a proposed lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct.

AA/SWA Ex. 1015, p.440 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

[0127] The format of the HTTP wrapper from the Member Agent to the VCN Manager is shown in FIG. 11. The wrapper includes an HTTP HEADER, XML HEADER and P-LENGTH fields. The HTTP header includes a POST HTTP field, an Identity field, a Content Type field, and a Content Length field. The XML header includes version information and packet type information. The Header includes error codes and explanations, as well as the content type and length.

[0128] The Registration exchange between the member agent and the VCN Manager is shown in FIG. 12A. When a Member Agent **565** attempts to register at step **1200**, Member Agent **565** will send a registration request packet **1202** to the VCN Manager **510** to start registration. The packet is included in an HTTP wrapper as illustrated at **1204**. The registration packet will carry the client Fully Qualified Domain Name (FQDN) and a Diffe-Hellman Key Exchange request to the VCN Manager. The packet further includes packet version information, type and length information, a user authenticator, the length of FQDN in octets, a VCN name offset, the member's FQDN in DNS format, the length of Diffe-Hellman value in octets, and the member's initial Diffe-Hellman value.

[0129] An Initial Password is passed to the user through an outside channel, such as e-mail (or other channel). In a setting where security is a concern, an alternative method such as personal communication or encrypted e-mail may be used.

[0130] The registration authenticator is computed using the first sixteen bytes of the HMAC-SHA-1 applied to the packet data with the password hash as the key. (Normally, the HMAC-SHA-1 algorithm generates a 20-byte result; in one embodiment of the system only the first (leftmost) 16 octets are used in the MAC.) The formulas are as follows: HMAC-Key-Field=SHA-1(Initial Password)Authenticator=HMAC-SHA-116(HMAC-Key-Field,Data)

[0131] The VCN Manager will respond in one of three ways **1206**, **1208**, **1212**, to the registration packet **1202**. VCN Manager **510** will acknowledge (ACK) the packet at step **1212** with the Registration Acknowledge (ACK) packet **1214** if the member belongs to a community but its status is "not registered." The VCN Manager also sends a phase-2 confirmation code to the member's e-mail address and changes the member status to "registering." The packet will transfer a "Time To Live" value to the member which is a timeout period in seconds for hearing back from the member with the confirmation code. Phase two of registration must be completed in this time period.

[0132] If the packet is abnormal (in size, FQDN length, bad type, etc.), the authenticator check fails, the member does not exist in the database, or the VCN server is not running, the VCN Manager drops the packet in step **1206**. The packet will be not-acknowledged (NACK) **1210** if the member is already in the "registered" state, the send e-mail operation fails, the process of updating the member to the "registering" state fails, or the random generator fails in attempting to generate a confirmation code in step **208**.

[0133] Upon receiving the Registration ACK **1214**, the user will send Registration File Request Packet **1220** to the VCN Manager **510** to start registration. This packet will transfer the following information to the VCN Manager: a registration file User Authenticator, the length of FQDN in octets, a VCN name Offset, and the member's FQDN in DNS format.

[0134] The registration file user Authenticator contained in the File Request packet **1220** is slightly different from the Registration Request Authenticator in packet **1202**, in that the Initial Password, passed to the user through an outside channel (e-mail for example), and the Confirmation Code, a temporary code sent in the second e-mail with a timeout to the user, are used: HMAC-Key-Field=SHA-1(Initial Password)User Authenticator=HMAC-SHA-116(HMAC-Key-Field,SHA-1(Confirmation Code)+Data)

[0135] The VCN Manager will send a Registration File acknowledge Packet **1230** to the member **565** in response to the Registration File Request packet **1220** in step **1228** if it is determined that the member belongs to a community. The Acknowledge Packet **1230** will transfer the following information to the member:

- Crypto Type—a code indicating how the rest of the packet is encrypted. This is provided in a crypto type field preceding the registration file.
- Registration File—a structure with a number of fields containing the information required by the member to successfully perform a join. It is sent encrypted using the key generated via the Diffie-Hellman key exchange.

[0138] A table representing the Registration File structure is shown in FIG. 12B. As shown therein, the Registration File contains an Authentication Type, a File Type, a File Length definition, a Token Key, a Key Timestamp, a Key Type, a Key Length, a High Availability (HA) Version, a HA Number, Server Information and Padding. The Token key is the shared secret with the server. The Token Key is identified by the Key Type, which is normally a Diffie-Hellman type in one embodiment. The VCN Manager also changes the member status to "registered."

[0139] If at step **1224**, the member agent status is not set at "registering," or the timeout for phase 2 has expired, a NACK packet **1226** is sent. If the packet is abnormal (in size, FQDN length, bad type, etc.), the authenticator check fails, or the user does not exist in the database, or the VCN server is not running, the packet is dropped in step **1222**. While current encrypting method for the file is to generate a key/IV pair from the combined Diffie-Hellman value using a Key Derivation Function, any number of suitable substitutes may be used.

[0140] In addition to the registration authentication described above, the system uses a packet authenticator to verify communications between the VCN Manager and Agents. The Authenticator is a cryptographically strong hash of the packet keyed by a shared secret between the source and destination. The authenticator is calculated over the entire packet using the HMAC-SHA-1 algorithm. The inputs to this Authenticator are not available until after Registration. As illustrated above, during registration an Authenticator based on the user password is used. The fields used in the calculation are a Diffie-Hellman Key comprising a multi-octet random string that is the result of the Diffie-Hellman key exchange protocol, and the entire packet data, with the Authentication field zeroed out.

[0141] The Authorization Key, AuthKey, described above, is derived from Diffie-Hellman using the KDF2 function, and used for general packet Authentication. AuthKey=KDF2 (Diffie-Hellman Key)MAC=HMAC-SHA-116(AuthKey, Data). The AuthKey need be calculated only once per registration from the KDF2 of the DH key and then stored for later use. It is known as the Authentication key and is 20 octets long.

Member Join/Leave

[0142] Once a user is registered, the user can join the VCN. Once joined, the user is a member of the VCN. Joining allows the user to let the VCN Manager and other members know that the user/member is on-line and available to communicate. The Join protocol runs between a Member Agent and the VCN Manager to establish a session key with the Manager, authenticate to the Manager, and make use of connections via the Route Directors in the community.

[0143] The Member Join process is illustrated in FIG. 13. There are two phases to the Join operation: phase one is an Initialize Request and phase two is the actual Join. At join time, the IPSec tunnel for secure communication is not established, so the first few join packets are sent outside the IPSec tunnel.

[0144] Initially, at **1302**, the Member Agent **565** will send an Init Request Packet **1304** to the VCN Manager **510** to start authentication. The packet will carry the following information to the VCN Manager:

- Version Variant Mask—used to indicate optional variations of the protocol from the member to the VCN;
- Token Timestamp—identifying when a Token Key was created (in seconds);
- Member seed—a random number to thwart so called "man-in-the-middle" attacks;
- Member Local IP—the member's Local LAN IP address; and

AA/SWA Ex. 1015, p.441 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

- Client FQDN—the client's fully qualified domain name.

[0150] Again, three responses **1306**, **1308**, **1312** are possible. At step **1306**, if the packet is abnormal, it will be dropped. Similarly, if the member fails authentication, at step **1308** a NACK packet **1310** will be sent.

[0151] If the member passes authentication at **1312**, the Manager will send an acknowledgement packet **1314** to Member **565**. An AuthKey is also transmitted as part of the INIT Request Packet, and the Manager authenticates the packet by checking this against a secure key digest. The acknowledgement packet **1314** packet will transfer the following information to the member:

- Version Variant Mask—version information;
- Member Seed—from the Init Request to protect against playback attacks;
- Manager Seed—a unique seed used to thwart man in the middle attacks;
- Session AH Key—used in IPsec;
- Session ESP Key—used in IPsec;
- Ink ACK Time—a time stamp used to tie this packet to the following Join Request. There is a timeout if the Join is delayed too long;
- Authentication Method—the method used for authentication;
- Route Director Private IP—if member is in a private network, this is the private IP address of the Private Route Director. The value is zero if no Route Director is used;
- Route Public Public IP—if member is in a private network, this is the public IP address of the Private Route Director. The value is zero if no Route Director is used;
- Tunneling Port—used for UDP encapsulation Route Director Flags. Only Bits **0** and **1** currently used to direct the agent to a Private Route Director, Network Route Director with UDP, or a Network Route Director with TCP.

[0162] At step **1312** of the join process, the VCN Manager will also determine whether the Member Agent attempting to join is behind a NAT device. The method by which this occurs is discussed below with respect to FIG. 21 and the results of this determination may force the Agent to negotiate a session with a Network Route Director which will provide a pseudo address value used as the Agent's local IP value in the Join request, discussed below. This process is discussed in depth with respect to FIG. 21.

[0163] Following receipt of the acknowledgement packet, at step **1316**, the member will send Join Request Packet **1318**. The packet's payload includes a manager seed, the initial ACK time, join flags, the member machine's local IP address (or pseudo address), the Route Director's private IP address, the Route Director's public IP, the member AH SPI and ESP SPI, the member listen port, a token timestamp, a GUID identifying the current client run, NetBIOS name support, a password hash, version information for high availability and security policy information.

[0164] In step **1320**, the VCN Manager will drop this packet if it is abnormal. In step **1322**, the VCN Manager will send a NACK packet **1324** if the member is not in the registered state, the timeout for Join from INIT ACK has expired, or updating the member to the Joined state fails.

[0165] If the join action succeeds, then in step **1326** the VCN Manager will send an acknowledge packet **1328**. The acknowledge packet payload includes the RMI Port at the VCN Manager, the Tunneling Port, VCN Manager Authentication Header (AH), Security Parameters Index (SPI) for IPsec, VCN Manager Encapsulating Security Payload (ESP) SPI for IPsec, the UTC Time (in seconds) when the member joined, VCN Manager Heartbeat interval (in seconds), the Member Heartbeat interval (in seconds), the VCN Manager's Virtual IP address, the Manager Subnet Prefix Length, the VCN Member Subnet Prefix Length, the Route Director's private IP address, the Route Director's public IP address, an indication of the updates that follow, an update of the Token Key, an update of the Security Policies, an update of High Availability indication, and padding. The member has now joined the community at **1330**. Once the member has joined, all communications can be encrypted using IPsec.

[0166] The system of the present invention also includes RADIUS authentication support. Generally, if a member attempts to authenticate using a RADIUS server, the VCN Manager will perform the same steps as when it receives the Join Request packet except for having a RADIUS server authenticate the member. The payload for this packet is similar to the Join Request packet except that it has an additional field for RADIUS password that is used by the RADIUS server to authenticate the member.

[0167] FIG. 14 shows the sequence for leaving a VCN. Initially, at step **1410** when a Member Agent is prepared to leave the community, a Leave Request Packet **1412** will be sent to the VCN Manager **510** to start the leave process. The Leave Request Packet will carry a Leave Flag, the FQDN Length, FQDN VCN Offset and Member FQDN. Unless dropped at step **1414** or a problem exists at **1416** which would generate a NACK packet **1418**, the VCN Manager will send the Leave ACK Packet **1430** to the member in step **1420**. This packet has no payload. At step **1440**, the member has successfully left the community.

DNS/Lookups

[0168] For one member to communicate with another member, the initiating member's agent will perform a query or DNS lookup (step **654** in FIG. 7) to determine the address of the other member, and then establish a secure communication channel between them.

[0169] The Member Agent utilizes the VCN Manager to perform lookups of other virtual members in the virtual community using DNS. The DNS operation is conducted using the DNS protocol with the VCN Manager. The member software sends a DNS query to the VCN Manager, and the manager returns information about the target member. Besides the target member's virtual IP address, the DNS response also contains additional information about the target member. While the VCN Manager accepts all DNS requests, it will only acknowledge the DNS requests of type A, which are targeted to virtual domain names in the secure virtual communities of the VCN Manager. The VCN Manager is the authoritative name server for those virtual domain names; other requests will simply be responded to with a "Server Failure."

[0170] The DNS query and response sequence is illustrated in FIG. 15. At step **1510**, a member will request a DNS lookup by sending a DNS request **1520** to port **53** of the VCN Manager. The DNS request **1520** will result in a normal DNS response **1575** unless any of a number of failure conditions are met, shown at steps **1522**, **1540**, **1550**, and **1560**.

[0171] If the Manager receives a query on port **53** that is not a DNS query, then at step **1522**, it is dropped. If, at step **1524**, the query is not a standard query, such as a DNS STATUS (a status lookup) or IQUERY (inverse DNS), or the class of the DNS query indicates an Internet (IN) query, or if the TYPE value of the request is a pointer (PTR) or host address (A), then, a "Not implemented" DNS response **1530** is sent over the virtual link to the Member Agent **565**.

[0172] At step **1540**, the VCN checks to see if the source IP address is for a member of the VCN. If the source IP address is not for a member of the VCN, the virtual IP look up fails or the type PTR query does not match, a "server failed" response **1545** is returned. At step **1550**, if there is no DNS Question section or there is another type of format error with the packet, a "format error" response **1555** is sent. The VCN determines whether the member has joined the VCN, at step **1560**. If not, a name error response is sent at **1565**.

[0173] If the name is a successful lookup (step **1570**), then the VCN Manager will send a DNS Response Packet **1575** to the member **565**. The response includes the following information: the target member FQDN; the target member virtual IP address; a source Route Director flag, the source member virtual IP address; the target member join time; the target member agent version; the target member private IP address; the target Route Director public IP address; the target member NetBIOS name; the shared key, shared by the two members; a target Ticket length; a target member Ticket

AA/SWA Ex. 1015, p.442 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

encrypted for target member only and containing a Ticket issue time, Ticket expiration time, and shared key; the target member virtual IP address, the source member virtual IP address, the source member private IP address; the source Route Director public IP address, the source member FQDN; and padding (to obtain a multiple of 16 octets). The Ticket provided by the DNS request is detailed further in the description of FIG. 16B.

[0174] The target member's virtual IP address will be presented using an A-type resource record in the answer section of the normal DNS response packet. All the remaining information will be transferred using a TXT-type resource record in an additional section of the DNS Response.

Encapsulation

[0175] Traffic between Member Agents in the VCN is encapsulated using UDP encapsulation. Encapsulated traffic between members can carry any IP traffic from any standard IPv4 compliant application. However, one port is set aside in the virtual network at the application layer to establish a connection between two members in the community. In one embodiment, this is UDP port **500**, which is set aside for Internet Key Exchange (IKE), allowing negotiation of an IPsec tunnel between the two members.

[0176] When an application on a member device wishes to open a connection to a peer on a target member device, a protocol is followed for the establishment of the IPsec session between the two. Member Agents are configured to listen on the UDP tunneling port (which defaults to port **20202**) for virtual traffic. As an accepted procedure non-IPsec traffic on the virtual IKE port **500** is accepted and passed to an IKE and Security Policy Module to allow for the possibility of initiating, an IKE exchange and the establishment of an IPsec session between the two members.

[0177] IKE is fully described in RFC-2409. IKE provides a key exchange with a peer and creates a security association (SA) for the IPsec module. IKE access between peers occurs in two phases: phase 1 establishes a secure, authenticated, channel with which to communicate, and phase 2, which negotiates a Security Association on behalf of IPsec. Phase 1 is generally referred to as the ISAKMP Security Association (SA) and includes a "Main Mode" and "Aggressive Mode." In one implementation, Aggressive Mode is used for phase 1. One of the allowed phase 2 exchanges is "Quick Mode" and in one implementation, Quick Mode is used in the system for phase 2.

[0178] FIG. 16B shows the aggressive mode IKE phase one exchange utilized in the present invention. FIG. 16A shows the standard aggressive mode IKE phase one exchange for comparison. In these figures, in accordance with standard IKE parlance, one device is considered an exchange "initiator" and the other a "responder".

[0179] In general, in phase one of the IKE exchange, peers are authenticated, an IKE Security Association (SA) policy between peers is established, a Diffie-Hellman exchange is performed to produce matching shared secret keys and a secure tunnel to negotiate IKE phase two parameters is established.

[0180] In FIG. 16A, an initiator exchanges a header (HDR), SA negotiation payload, Key Exchange (KE), nonce payload (Ni, where "i" indicates an "initiator" payload) and identity of the party (IDii). The key exchange payload contains the public information exchanged in a Diffie-Hellman exchange. The responder returns the HDR, SA, KE, a responder nonce payload (Nr), its identity (IDir) and the HASH responder (HASH_R) payload, which is generally a hash of the ID payload and is used to authenticate the exchange. The initiator returns the HDR and HASH initiator (HASH_I) payload, and the initial secure tunnel is established.

[0181] In accordance with the present invention, FIG. 16B illustrates the use of an extension to aggressive mode exchange. This is performed by adding a ticket payload (TKT*) to distribute a shared-key to remote peers.

[0182] The Ticket is the means by which one Agent can identify whether another Agent is a trusted member of the virtual community. Essentially, the Ticket includes information identifying the initiating member to the receiving member.

[0183] The ticket is issued by the VCN Manager and encrypted for the receiving member with a member-server shared secret; only the receiving member can open it. The ticket contains a time-stamp, a sequence number and a shared-secret used for IPSEC between the two members. To communicate with the receiving member, the initiating member obtains the ticket from the VCN Manager (through, for example, the DNS sequence, described above) and passes it to the receiving member in a payload that can ride on an IKE packet. The receiving member receives the Ticket, decrypts the Ticket using the member-server shared secret, and uses the information in the Ticket to establish secure communication with the initiating member.

[0184] This payload, TKT, is formatted as shown in FIG. 17. The packet **1700** contains an IP header **1710**, UDP header **1720**, System shim **1730**, and Virtual IKE Phase 1 UDP/IP packet **1740**. FIG. 18 illustrates the structure and data of an exemplary first packet **1740**. The IKE Ticket Payload in the first IKE packet contains information on the payload and the payload data, including the type of payload following next and the ticket payload data **1756**. The payload data **1750** includes the size, number and item list **1766**. The item list **1760** includes type, size and item information. The IKE ticket payload data **1740** contains the item types

[0185] The item types **1770** are shown in the last table of FIG. 18: "My FQDN"—a null terminated FQDN in label dot format. (For example, a human readable FQDN "bob.system.com" is encoded as "bob.system.com\0x00.") My Ticket data which includes a Manager Current Time (UTC of Manager as known by initiator); and an Initiator Virtual IP (Obtained at Join time) Target Virtual IP (Obtained from Manager) and Padding. The Peer FQDN Format is a null terminated FQDN in label dot format. For example, a human readable FQDN "bob.system.com" is encoded as "bob.system.com\0x00". Finally, the Peer Ticket data includes: a Ticket Issue Time (UTC (seconds) on VCN Manager); a Ticket Expiration (UTC (seconds) for ticket expiration); a Shared Key used by the two Members for IKE; a Target Virtual IP Address; the Initiator NAT Port; the Initiator Subnet; the Initiator Virtual IP Address; Initiator Private IP Address, the Initiator Public IP Address, the Initiator FQDN and padding.

[0186] The Diffie-Hellman key exchange protocol is utilized in the Internet Key Exchange (IKE) protocol that precedes IPsec. The prime and generator value are taken from a well-known Internet Draft entitled, "More Diffie-Hellman groups for IKE," Kivinen et al., IP Security Protocol Working Group (IPSE) Internal Draft, Dec. 13, 2001, for proposed use within the Internet Key Exchange (IKE) protocol.

Administrative Functions

[0187] The system can simulate pings to any of the Route Directors (NRD or PRD). This ping is sent inside a packet generated from an application used to trouble-shoot the virtual network by touching the Route Directors and insuring that they are alive.

[0188] An exemplary ping process is illustrated in FIG. 19. As shown therein a pinging application **1902** at step **1904** sends a ping request packet **1906** to the Route Director **560**. The Route Director receives the ping at **1910** and generates a response at step **1912**. The ping response packet **1914** is returned to the application **902** at step **1916**.

[0189] The ping request packet is sent and returned on the default tunneling UDP port (which in FIG. 5B is UDP Port **20202**). The Ping Request **1906** packet is formatted as shown in FIG. 19, with the content of the shim and the ping packets exploded in further detail. In the shim **1930**, the source and destination Route Director public IP addresses (gIP) and private IP addresses (pIP) are all set to 0. In the system ping field **1960**, the ping type field may be a ping request or a ping response. The Sequence field in the response is set to the same value as the Sequence field in the request packet.

[0190] Another function which may be performed is an Agent Query. FIG. 20 illustrates a query request from a Member Agent requiring system/status information of another member. The first Member Agent **565** at step **1802** will send a Query Request Packet **1810** to the VCN Manager **510**. The Packet contains definitions for the Maximum Number of Records to return, a status Mask indicating whether the members are registered and/or joined, a

AA/SWA Ex. 1015, p.443 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

platform Mask, indicating the platform (desktop, server, laptop, mail server, etc) of the member, the FQDN Length, FQDN VCN Offset, Search String Length, Member FQDN and a Search String for pattern matching. This packet is sent over the IPsec tunnel between the VCN Manager and the Member Agent.

[0191] If the packet is abnormal it is dropped at step **2012** if there is an error in the query authentication file or the member is not joined, NACK **2016** is sent in step **2014**. If the packet is not abnormal, no error is present, the member passes authentication and was joined, then the VCN Manager sends a query acknowledgement Packet **2030** to the member. The packet payload includes a number of records with the following fields: the status of the member, the platform type of the member, and the member's FQDN String. Note that the FQDN is null-terminated and consistent with the FQDN in DNS format definitions. Here, a human readable FQDN "www.abcdefg.com" is encoded as "www.abcdefg.com\0x00".

[0192] Each joined member will periodically send a heartbeat packet to the VCN Manager so that the VCN Manager can determine if the member is alive. In addition, the member's heartbeat packet is used to determine how long the member is actually joined. This information can be used to allow a provider of the infrastructure for the system to generate revenue from users on a per-use time basis. Conversely, the VCN Manager periodically sends its heartbeat packet to joined members so that the joined members can know if the Manager is alive. This can be used by the member to determine if it should switch to a backup VCN Manager. Heartbeat packets are sent inside the system tunnel on the default tunneling port (UDP port **20202**) and are IPsec protected.

Route Directors

[0193] Route directors allow communication to a member that is in a private network. The PRD resides within a private network, behind the NAT device. The NRD resides on the public side of the NAT device. The NAT device can be a Network Address Port Translation (NAPT) NAT device or a basic NAT where only addresses are translated.

[0194] Note that devices with public addresses do not require Route Directors (RDs). In the context of FIG. 5B, devices M_A and M_E do not require either a PRD or NRD, since they reside in the public address space. Likewise, M_X does not require the PRD for its domain **540**, since it has a public address (or is statically mapped to a public address at the NAT device **515**).

[0195] The NRD implements a NAT traversal architecture which allows System packets to enter and exit a private network. The NRD maintains persistent connections/sessions with members that are behind NAT devices. Member Agents initiate a TCP or UDP persistent connection/session with the NRD and use keep-alive messages to ensure that the NAT device does not drop the member's connection/session. The use of TCP or UDP is based on a bit set by the VCN Manager in the INIT ACK packet of the Join Protocol. Communication to a member uses NRD tunnels between the NRD and the Member Agent through the persistent connection/session. More information about a suitable NAT traversal architecture is found in U.S. Pat. No. 7,139,828 and U.S. patent application Ser. No. 10/233,288, "Communicating With An Entity Inside a Private Network Using an Existing Connection to Initiate Communication," both of which are incorporated herein by reference.

[0196] When a member behind NAT attempts to join a virtual network by contacting the VCN Manager as discussed above, the VCN Manager will detect the presence of the NAT device, direct the member to a specific NRD and indicate the use of TCP or UDP. The presence of the NAT device must be detected during the initialize Init message portion of the join sequence so the VCN Manager can inform the member that it needs to setup a session with the assigned NRD prior to the Join message sequence.

[0197] In one embodiment, the NRD uses a pseudo address. The pseudo address is different than the virtual address and is used solely for NRD routing. The pseudo address assigned by the NRD will allow the NRD to map a packet to the member's post-NAT IP address and UDP port.

[0198] The process for establishing a session with a NRD and obtaining an address therefrom is shown in FIG. 21. Initially (as described in FIG. 13), a member behind a firewall will send an init request **1304** to VCN Manager **510**. In addition to the functions performed with respect to step **1306**, **1308**, and **1311** (of FIG. 13), the VCN Manager will detect that the member is behind a NAT device and whether it is served by a PRD in step **2120**.

[0199] The detection of a NAT device is accomplished using a field with the member's local IP address in the Init packet sent to the VCN Manager. The VCN Manager detects the fact that Agent **565** is behind a NAT device by comparing the member's private IP address in the INIT message payload with the source address in the TCP/IP headers. If the addresses differ, then a NAT device is present. At step **2120**, the VCN Manager must next check if the member's NAT device is associated with a known PRD (Premises Route Director). If no PRD is found, then the VCN Manager will check if the member can use a known NRD. If an NRD is found then the INIT ACK **1314'** will indicate that the member must establish a session with the NRD prior to joining the VCN. If the NRD can support TCP tunneling, the INIT ACK will also indicate to the member to start a TCP connection rather than a UDP connection. If neither a PRD nor an NRD is found for the private member, an Init NACK will be returned. The VCN Manager will find an available NRD and send an INIT ACK **1314'** with the NRD info data contained therein. The contents of an INIT ACK packet **1314** are discussed above with respect to FIG. 13.

[0200] At step **2132**, the member will seek to establish a session with the NRD and will send address request **2130** to the NRD. The member sends the Address Request Packet **2130** to the NRD. The packet includes an IP Header, UDP Header or TCP header, and Shim. In this case, the shim includes the NRD's public address. At step **2135**, the NRD assigns the member a pseudo address. This is used as the member's private address in the Shim when external members send packets to the NRD for forwarding to the private member. The NRD will store the association of the pseudo address with the Member's NAT device public address and port number. When other members of the VCN perform a DNS request on the member behind the NRD, as part of the DNS response, they will receive the public address of the NRD and they will receive the pseudo address as the private address for the member behind the NRD. When sending a communication to the member behind the NRD, the outer packet will be addressed to the public address of the NRD. The NRD will access the shim to identify the pseudo address. The NRD uses the pseudo address as a handle to the persistent connection/session when sending packets through a NAT to the member. Once identifying the appropriate persistent connection/session, the shim and virtual packet are encapsulated and sent to the destination, via the NAT device, using the identified persistent connection/session. When the NAT device receives the message, it will do the address and port translation, and forward the message to the member agent's real local address and port on the private network.

[0201] In one aspect, the pseudo address comprises portions of the public IP address space in IP version 4 that had been reserved for special purposes. This ensures that no machine within a private realm will have the same pseudo IP address as the private address of a machine in any separate and distinct private realm. In order to prevent this from happening, the system of the present invention uses addresses that are otherwise not used or reserved. Examples include the 0.0.0.0, the 10.0.0.0, 14.0.0.0, 127.0.0.0, 169.2454.0.0, 172.16.0.0 and the like.

[0202] The NRD provides the pseudo address to the Agent **565** in a NAT Traversal Address Response Packet **2140**. The packet includes a shim having an indicator that the response is a pseudo address response, as well as the source Route Director public IP address and Destination Route Director public IP address, (which is set equal to the NRD address), the Source member private IP address (0) and the Destination member private IP address, which is the Virtual IP. Hence all communications for the Member Agent will be routed to the NRD **520**. After acquiring the pseudo address from the NRD, the member designates that pseudo address to the VCN Manager as its local address in Join packet **1318**.

[0203] Note that there is an extra packet exchange **2145**, **2150** when establishing a TCP connection that is not required when establishing a UDP connection with the NRD. This packet is the NRD Init Request Packet **2145**. The previous TCP session for the Address Request and Address Response must be closed and a new TCP session opened which will remain open for the duration of the tunnel session. The member sends the Init Request message to the NRD as the first message in this TCP session. This message only has a TCP header and System Shim preamble, and has no data following the Shim.

AA/SWA Ex. 1015, p.444 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

[0204] After receiving the pseudo address, the join process completes with the join request packet **1318**, and join ack packets **1328**. After the join processing is complete, TCP/UDP encapsulated traffic flows between the member and the NRD through the NAT. The member is now ready to establish connections with other members.

[0205] When outbound System traffic from a member behind a NAT device to the NRD is not frequent enough to keep the NAT device's mappings active, the member may to send keep alive messages to the NRD's TCP port **80** or UDP encapsulation port to ensure that the NAT device does not drop the TCP/UDP encapsulation session. The member sends this message to the NRD to ensure that the NAT device does not drop the TCP/UDP port mapping. The keep-alive messages do not need to be sent when other messages were sent out during the keep-alive interval.

[0206] The member sends this NAT Traversal Leave Packet message to the NRD to release the session and pseudo address when the member is leaving the VCN. The NAT traversal switch will verify that the receive-from socket address this message came from matches the lookup table entry before deleting the member's address.

Group Agent

[0207] For some devices, member client software cannot be installed on the device or it is not desirable to install member client software on the device. For example, a printer or other networked devices may not be able to load software. For various reasons, some entities may not desire to add network software onto their machines. Additionally, some devices may use operating systems that do not support running the member agent software. For those devices that cannot or choose not to use member agent software, a Group Agent can be used. The Group Agent acts as a proxy for one or more members of a VCN without requiring installation of member agent software on the client devices. Thus, a device can become a member of a VCN without changing any of the software on the device by using the Group Agent.

[0208] FIG. 22 is a block diagram depicting various components of the present invention utilizing a Group Agent. Note that some of the members of a VCN can use a Group Agent while other members do not use a Group Agent. FIG. 22 shows ten devices M_1-M_{10}. Devices M_1, M_2, M_3, M_4 and M_{10} are devices that are participating in the VCN without using member agent software. Rather, they will use a Group Agent. Devices M_5, M_6, M_7, M_8 and M_9 are devices which include member agent software and, therefore, do not need to use a Group Agent. FIG. 22 shows some of the many varieties of permutations of using Group Agents, Network Route Directors and Private Route Directors. Other permutations can also be used with the present invention. Also note that FIG. 22 is more of a structural view of additional components of the present invention, as compared to FIG. 5B which is more of a symbolic/logical view.

[0209] FIG. 22 includes a first private network which connects to the Internet (or other network) via NAT device **2202**. In addition to NAT **2202**, the private network includes device M_1, device M_2 and Group Agent **2204**. In one embodiment, the Group Agent runs on the same machine as a Private Route Director. Devices M_1 and M_2 do not include agent software. Rather, they participate in the VCN using Group Agent **2204**.

[0210] A second private network allows devices to communicate to the Internet (or other network) via NAT device **2210**. That private network also includes Group Agent **2212**, device M_3 and device M_4. Note that Group Agent **2212** does not include a Private Route Director. Thus, for devices M_3 and M_4 to be reached by other members of the VCN, communication is performed via Network Route Director **520**. In one embodiment, each of the private networks are different physical address realms. That is each uses a different set of private IP addresses. The present invention will also work if the private networks have overlapping addresses. That is, one or more private IP addresses are used by more than one private network involved in a VCN.

[0211] A third private network, which includes devices M_5 and M_6, provides for communication on the Internet via NAT device **2220**. A fourth private network, which includes devices M_7 and M_8, allows its components to communicate on the Internet (or other network) via NAT device **2230**. This fourth private network includes Private Route Director **2232**. Because devices M_7 and M_8 include member agent software, there is no need for a Group Agent on this network. Device M_9 has a public IP address and includes member agent software; therefore, it communicates and participates in the VCN as described above. Device M_{10} has a public IP address; however, device M_{10} does not include member agent software. For device M_{10} to participate in the VCN, it must make use of Group Agent **2234**, which has a public IP address.

[0212] In one embodiment, a Group Agent includes software running on a computing device, including (but not limited to) a server, router, personal computer, minicomputer, mainframe, mobile computing device, or other suitable computing device. In other embodiments, the Group Agent, or any other of the software components described above, can be performed by its special purpose computing device.

[0213] A Group Agent acts as a proxy for one or more members which do not have member agent software. For example, Group Agent **2204** is a proxy for devices M_1 and M_2; and Group Agent **2212** is a proxy for devices M_3 and M_4. Group Agent **2234** is a proxy for device M_{10}. Although FIG. 22 shows the Group Agents being proxies for one or two members, a Group Agent can be a proxy for more than two members.

[0214] Communication between two members of a VCN can pass through two NAT devices, one NAT device for each member. For example, communication between device M_1 and device M_4 will pass through NAT device **2202** and NAT device **2210**. Additionally, communication between device M_1 and another entity in a private network configured like the private network of device M_1 will require communication to pass through two NAT devices.

[0215] Note that a single Group Agent can participate in more than one VCN. For example, Group Agent **2204** can be used to allow device M_1 participate in a first VCN and concurrently (for all or part of the time) allow device M_2 to participate in a second VCN. Because there can be multiple virtual community networks, the VCN Manager is able to create and maintain, the multiple virtual community networks. As described herein, the VCN Manager identifies which entities can communicate on each VCN by maintaining a list of domain names for each VCN. For example, one list may include the domain names for devices M_1-M_{10}.

[0216] The Group Agent requires initialization so it may know which members it is a proxy for. Group Agent initialization cannot occur until after the Group Agent has joined the VCN Manager as a member. The join prior to Group Agent initialization is for a pseudo-member so the proxy initialization messages can use virtual IP addresses and the tunneling protocols described above to travel on an IPsec tunnel between VCN Manager **510** and the particular Group Agent. Separate member specific tunnels will be created when the Group Agent later joins for the proxied members. The Group Agent join will require the Group Agent to be registered with the VCN Manager. In one embodiment, this registration will be done during the installation of the Group Agent.

[0217] FIG. 23 provides a flowchart describing one embodiment of the process for Group Agent initialization. In step **2302**, the Group Agent joins as a pseudo-member. This process of step **2302** is performed as described above. In step **2304**, the Group Agent will send an initialization request to the VCN Manager. The initialization request is a packet that includes the fully qualified domain name for the Group Agent, a packet version indication, a packet type indicating that it is an initialization request, a packet length, and an authentication code. If the received initialization request is abnormal (step **2306**), then the initialization request is dropped in step **2308**. If the packet was normal but authentication failed (step **2312**), then the VCN Manager sends a NACK to the Group Agent in step **2314**. If authentication was successful and the initialization request was normal, then the VCN Manager sends an acknowledgement to the Group Agent in step **2320**.

[0218] After completion of step **2320**, the Group Agent is initialized and now must join each of the members it is proxying. To do so, the Group Agent will perform a loop where each iteration will include joining for one of the members that is being proxied. In step **2322**, it is determined whether there are any more members being proxied that have to be joined. If there are more members to join, then the Group Agent will join for one member being proxied in step **2324** and the method will loop back to step **2322**. When there are no more proxied members to be joined, the process of FIG. 23 is

AA/SWA Ex. 1015, p.445 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

complete (step **2330**). The process of joining for a proxy member is the same as the process of joining described above; however, the process is performed for the member by the Group Agent rather than by the member agent. The virtual IP address received by the Group Agent is for the member being proxied. The Group Agent stores that virtual IP address in a data structure for the member. In one embodiment, there is a separate data structure for each member being proxied. In another embodiment, there is one data structure which has separate records for each member being proxied. This data stored will include the member's virtual IP address and private address in the local LAN, as well as other information that will be described below.

[0219] The acknowledgement sent from the VCN Manager to the Group Agent in step **2320** contains all of the member information required so the Group Agent can send the appropriate join requests for each member being proxied. The following information is in the acknowledgement sent from the VCN Manager to the Group Agent: packet version indicating the version of the header, packet type indicating that it is a acknowledgement, packet length, authentication code, subnet IP address, subnet prefix, public IP address of the Private Route Director (when the Group Agent also includes a Private Route Director), Private Route Director ping flag (1 if PRD responds to pings), the number of members being proxied, the number of permanent connections from proxied members to other members that the proxy must make, the member record list and the connect record list. The member record list is a set of records for each member being proxied. The following information is stored in each record: member password (password SHA1 digest), member's local private IP address, the length of the member's fully qualified domain name, the member's fully qualified domain name, offset to the VCN name, authentication type (0=preshared 1=certificate), time stamp indicating when the token key was created, token length in bytes, token key (member shared secret with VCN Manager), HA version number, number of HA records, HA record list and authentication key (generated by server for the proxy). Each HA record in the HA record list includes a VCN Manager IP address for the next VCN Manager, a join port for the next VCN Manager and a service port for the next VCN Manager in case the current VCN Manager goes down. The connect record list includes the following three fields: proxy member index (zero based index into member list), DNS request length and a DNS request.

[0220] Once the Group Agent joins for all of its members, then any of its members can receive communication from other members of the VCN or can initiate communication to other members in the VCN. Members that are being proxied by a Group Agent can communicate with other members being proxied by the Group Agent, with other members proxied by a different Group Agent (regardless of whether they are in a private network or available on the public Internet), and members that do not use a Group Agent (regardless of whether those other members are in a private network or available on the Internet with a public IP address), as long as they are all members of the same VCN. From the point of view of an application on a member being proxied by the Group Agent, the VCN appears as a local subnet (or LAN) and all of the members of the VCN appear to be on the local subnet (or LAN). However, the VCN is not a local subnet (or LAN); rather it is a virtual subnet (or LAN). Each of the members of the VCN will have a Virtual IP Address on the virtual subnet.

[0221] Because members of a VCN register with the VCN Manager, the VCN Manager will know how to find the members (e.g. it will know its public and private addresses). Thus, a Group Agent acting as a proxy for a first member will be able to act as an intermediary for that first member when talking to a second member of a VCN even if the second member moves to a different or new private network and/or changes its IP address. That is, when the second member makes the move or change, the second member will so inform the VCN Manager. The VCN Manager will inform the Group Agent of the change so that the Group Agent can continue to act as an intermediary between the first member and the group member. More information about communicating with mobile entities can be found in U.S. Pat. No. 7,139,828; U.S. patent application Ser. No. 10/161,573, "Creating A Public Identity For An Entity On A Network," filed on Jun. 3, 2002; and U.S. patent application Ser. No. 10/233,288, "Communicating With An Entity Inside A Private Network Using An Existing Connection To Initiate Communication," filed on Aug. 30, 2002, all three applications are incorporated herein by reference in their entirety.

[0222] FIG. 24 is a flowchart describing one embodiment of a process for initiating communication with a member that is being proxied by a Group Agent. In FIG. 24, the communication is being initiated by a member that is not being proxied by a Group Agent. That is, the member initiating communication is a member that has agent software loaded on it. That member is initiating communication with a member that does not have agent software. Prior to the process of FIG. 24 being performed, the Group Agent has joined the member into the VCN and the member initiating communication has already joined the VCN. For example purposes, looking at FIG. 22, the process of FIG. 24 can be performed by M_5, M_6, M_7, M_8 or M_9 initiating communication with any of devices M_1, M_2, M_3, M_4 or M_{10}. Assume, for example purposes, that device M_9 is initiating communication with device M_1. The destination device is also assumed to be served by a Private Route Director.

[0223] In step **2402**, an application on the source device (e.g., device M_9) is intending to send a message to an application on the destination device (e.g., device M_1). In step **2404**, the application on the source device sends a DNS request to the VCN Manager using the domain name of the destination. For example, the application on M_9 will send a DNS request using the domain name for M_1. In step **2406**, the VCN Manager returns a response to the DNS request. This response includes the public IP address for private Route Director **2204**, the private IP address for member M_1 and the virtual IP address for member M_1. In some embodiments, the DNS response also includes a token key (as described above). The Agent on the source device (e.g., M_9) stores the information it received from the VCN Manager. In step **2410**, the Agent on the source device returns the virtual IP address for the destination to the application which initiated the DNS request. In step **2412**, the application on the source device initiates the sending of a message to M_1 using the virtual IP address. That is, a virtual IP packet is created where the source address is the virtual IP address for the source machine (M_9) and the destination address in the virtual IP packet is the virtual IP address for the destination device (device M_1). The virtual IP packet is created in step **2414** and subject to IPsec (or other security means). In step **2416**, the virtual IP packet is encapsulated. Encapsulation includes adding a shim, a UDP header and an IP header, all as described above. The shim includes the public IP address for the Private Route Director associated with the destination member (e.g., PRD **2204**) and the private IP address for destination (e.g. member M_1). If the source, the member initiating communication was in a private network, then the shim would also include the public IP address for the Route Director associated with the source and the private IP address for the source. In step **2418**, the encapsulated packet is sent to the NAT for the destination's private network. That is, in the example above, the newly created packet is sent to NAT **2202** via the Internet (or other network). In step **2420**, the encapsulated packet is sent from the NAT (e.g., NAT **2202**) to the Route Director for the destination (e.g., PRD **2204**).

[0224] In step **2422** of FIG. 24, the Route Director removes the virtual IP packet and the shim from the encapsulation and presents both the virtual IP address and the shim to the Group Agent (e.g., Group Agent **2204**). The Group Agent stores the information from the shim, as described above with respect to the member agent software. In one embodiment, the Group Agent includes the necessary logic to received the communication so that no route director is necessary. In step **2426**, the Group Agent extracts the virtual IP packet from IPsec. In step **2428**, the Group Agent chooses a private IP address for the source entity. In the above example, the source entity is device M_9. Group Agent **2204** will pick a private IP address that is routable in the private network associated with device M_1 and NAT **2202**. This private address will be used by device M_1 to identify M_9. In step **2430**, the Group Agent will change the source address in the virtual packet. That is, the virtual packet originally had a source address equal to the virtual IP address for the source device (e.g., M_9) and a destination address equal to the virtual IP address for the destination device (e.g., M_1). In step **2430**, the source address in the virtual IP packet is changed to be equal to the private IP address chosen by the Group Agent for M_9 in step **2428**. In step **2432**, the Group Agent changes the destination address in the virtual IP packet to be equal to the private IP address in the local LAN for M_1. In step **2434**, the packet is sent by the Group Agent to the destination machine (e.g., sent to M_1).

[0225] The above discussion of FIG. 24 was made with respect to the example that the communication has been initiated by device M_9 which is a member having a public IP address and member agent software. The process of FIG. 24 can also be performed by a member which does not have a public IP address, including members using a Private Route Director and/or a Network Route Director. When the process of FIG. 24 is being performed by members using Route Directors, the shim that is added to the encapsulated packet in step **2416** includes the private IP address for the member and

AA/SWA Ex. 1015, p.446 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

the public IP address for the Route Director. The example used in discussing FIG. 24 also assumes that the destination was a device in a private network where the private network included a Group Agent and a Private Route Director. The process of FIG. 24 can also be adapted to work with a member using a Group Agent where the member has a public IP address and/or a member in a private network that uses a Network Route Director.

[0226] When sending communication to an entity with a public IP address that uses a Group Agent, the shim will include the public IP address for the Group Agent and the public IP address for the member in step **2416**. The packet will not be sent to a NAT or to a Route Director. Rather, the packet will be sent directly to the Group Agent. The Group Agent will access the virtual IP packet in step **2426**. Rather than choosing a private IP address to identify the source, the Group Agent will choose a public IP address for the destination to use to refer to the source. The virtual IP packet will be changed so that the source address is equal to the public IP address chosen by the Group Agent to represent the source and the destination address will become the public IP address for the destination. The virtual IP packet (which is no longer virtual) will be sent to the destination.

[0227] If the destination member participates in a VCN using a Network Route Director (e.g., device M_3 using NRD **520**), then the encapsulated packet is sent to the Network Route Director in step **2418**. The Network Route Director will communicate the shim and virtual IP packet to the Group Agent (e.g., Group Agent **2212**) via a persistent connection as described above in FIG. 7, steps **673-675**, **677**, except that the packet is forwarded to the Group Agent rather than the NAT device. The Group Agent will then perform steps **2424-2434**, as described above.

[0228] FIG. 25 is a flowchart describing one embodiment of a process for the destination device responding to the initiation of communication from the source device. In the example discussed above, this process would include device M_1 responding to device M_9. In step **2502**, the application on device M_1 attempts to send a communication. A packet is then created using the private addresses. The packet would include a source address equal to the private IP address in the LAN for device M_1. The destination address would be equal to the private IP address in the LAN that is used to identify device M_9. That packet is sent to the Group Agent in step **2504**. In step **2506**, the Group Agent changes the packet by replacing the private addresses with virtual addresses. The source address is replaced with the virtual IP address in the VCN used to identify device M_1. The destination address in the packet is replaced with the virtual IP address in the VCN used to identify device M_9. In step **2508**, this packet is subject to IPsec, and encapsulated as described above.

[0229] In step **2512** of FIG. 25, the Group Agent sends the packet. In the example above, the Group Agent would send the encapsulated packet to device M_9 using the public IP address for device M_9. If the Group Agent is sending the packet to a member that is in a private network, then the encapsulated packet would be sent to the Group Agent/Private Route Director for the member or to the Network Route Director for that member. If the responding device (e.g. M_1) is using a Network Route Director, then the Group Agent can still send the reply packet directly to the original source without going through the Network Route Director. If the replying device (e.g. M_1) has a public IP address, then the packet sent to the Group Agent would include the public IP addresses for the responding device and the public IP address that the Group Agent told the replying device to use to identify the original source device. In one embodiment, when the member using the Group Agent has a public IP address, an IPsec tunnel can be created between the Group Agent and the member device.

[0230] FIG. 24 contemplates communication being initiated by a device that has member software loaded on it. FIG. 26, on the other hand, describes a process that is performed when communication is initiated by a device that does not have member software and, therefore, uses Group Agent software. In step **2602**, the application on the initiating member will send a DNS request. This DNS request will be sent to the Group Agent. The Group Agent receives the DNS request in step **2604**. In step **2606**, the Group Agent sends its own DNS request for the same domain name to the VCN Manager. In step **2608**, the Group Agent receives a response from the VCN Manager. This response will include the virtual IP address for the target, the public IP address of the Route Director for the target (if any) and the private IP address for the target (if any). If the target has a public IP address, then the public IP address will be returned. In step **2610**, the Group Agent will choose a private IP address in the local LAN to be used to identify the target. The virtual IP address returned from the DNS request will be mapped to this private IP address in the local LAN. In step **2612**, the Group Agent will return that chosen private IP address to the application as a response to the application's DNS response. In step **2614**, the application will initiate the communication. In one embodiment, the process of **2614** includes performing the steps of FIG. 25. Note that if the member who is initiating the communication in the process of FIG. 26 has a public IP address, rather than being in a private network, then in step **2610** the Group Agent will map the virtual IP address to a public IP address that the Group Agent and member will use to identify the target. It is this mapped public IP address that is returned to the application in response to the DNS request. The mapped public IP address is routable to the Group Agent.

[0231] Although the Group Agent is described above with respect to use with a VCN, the technology of the Group Agent is broader than a VCN. Thus, the Group Agent can be used to allow entities to participate in other types of networks, communities, groups, organizations, communications, etc.

[0232] Note that in one embodiment, the member being serviced by the Group Agent must be in the same physical address realm as the Group Agent. In this manner, the Group Agent is used to bridge that physical address realm with the virtual space. The Group Agent contains the functionality to allow the member to participate in the virtual community; however, all the protocols of the virtual community terminate at the Group Agent. This way, the member receives a normal IP packet. From the point of view of the member, the Group Agent works like a router which connects the member to the subnet of virtual nodes.

[0233] The foregoing detailed description of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. For example, any number of VCN Managers may be used. Any combination of NRDs and PRDs may be used to improve network efficiency. Any combination of Member Agents and Group Agents may be used, and the Virtual Community may be of any size. Additionally, while the above description provided an example using the protocols and addressing currently used on the Internet, the present invention can be used with other protocols and addressing schemes. The described embodiments were chosen in order to best explain the principles of the invention and its practical application to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the claims appended hereto.

Original

Classifications

IPC	CPC	US Class	ECLA
G06F15/16	G06Q10/109	709/245	G06Q10/109
G06Q10/10	G06Q30/02	726/15	G06Q30/02
G06Q30/02			

AA/SWA Ex. 1015, p.447 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Persons

Ultimate Owner

Original
F. Poszat Hu {/api/control?client=&query=uo:("F.%20Poszat%20Hu")&autosearch=true)

Original Assignees

Original	Standardized	Normalized
Hasan S. Alkhatib {/api/control?client=&query=pa:("Hasan%20S.%20Alkhatib")&autosearch=true) Saratoga, California, United States of America, US		
Fouad A. Tobagi {/api/control?client=&query=pa:("Fouad%20A.%20Tobagi")&autosearch=true) Los Altos, California, United States of America, US		
Farid F. Elwailly {/api/control?client=&query=pa:("Farid%20F.%20Elwailly")&autosearch=true) San Jose, California, United States of America, US		

Current Assignees

Original	Standardized	Normalized
INPRO NETWORK FACILITY, LLC {/api/control?client=&query=pacu:("INPRO%20NETWORK%20FACILITY%2C%20LLC")&autosearch=true) 2711 CENTERVILLE ROAD, SUITE 400, 19808, WILMINGTON, DELAWARE, UNITED STATES OF AMERICA	INPRO NETWORK FACILITY {/api/control?client=&query=pacus:("INPRO%20NETWORK%20FACILITY")&autosearch=true)	
INTELLECTUAL VENTURES I LLC {/api/control?client=&query=pacu:("INTELLECTUAL%20VENTURES%20I%20LLC")&autosearch=true) 251 LITTLE FALLS DRIVE, 19808, WILMINGTON, DELAWARE, UNITED STATES OF AMERICA	INTELLECTUAL VENTURES {/api/control?client=&query=pacus:("INTELLECTUAL%20VENTURES")&autosearch=true)	INTELLECTUAL VENTURES {/api/control?client=&query=pacun:("INTELLECTUAL%20VENTURES")&autosearch=true)

Inventor(s)

Original
Hasan S. Alkhatib {/api/control?client=&query=in:("Hasan%20S.%20Alkhatib")&autosearch=true) Saratoga, California, United States of America, US
Fouad A. Tobagi {/api/control?client=&query=in:("Fouad%20A.%20Tobagi")&autosearch=true) Los Altos, California, United States of America, US
Farid F. Elwailly {/api/control?client=&query=in:("Farid%20F.%20Elwailly")&autosearch=true) San Jose, California, United States of America, US

Legal representative(s)

Original	Standardized	Normalized
McAndrews, Held & Malloy, Ltd. {/api/control?client=&query=ag:("McAndrews%2C%20Held%20%26%20Malloy%2C%20Ltd.")&autosearch=true)		

Legal information

Standardized Post issuance INPADOC

AA/SWA Ex. 1015, p.448 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

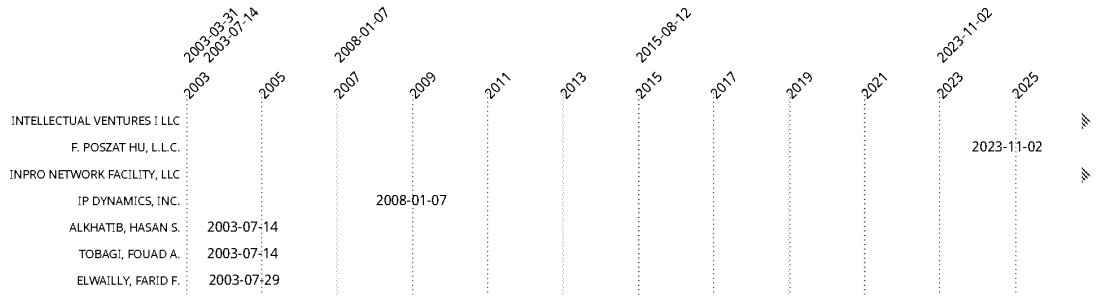
Legal status

Event	Date	Description
Granted	2011-05-24	GRANTED
Filed	2003-03-31	FILED

Designated states

Date	Event code	Description

Ownership



Payment status

Date	Status	Event code	Description
2022-10-12	Fee paid	M1553	PAYMENT OF MAINTENANCE FEE, 12TH YEAR, LARGE ENTITY.
2018-10-16	Fee paid	M1552	PAYMENT OF MAINTENANCE FEE, 8TH YEAR, LARGE ENTITY.
2014-10-28	Fee paid	M1551	PAYMENT OF MAINTENANCE FEE, 4TH YEAR, LARGE ENTITY.

Litigation/Opposition

Docket number	Docket description	Court	Date Filed

No CourtLink®

Pharmaceuticals

Product	Type	Active Ingredient	Applicant	Application No.	Application Type	Approval Date	Patent Expiry Date	Patent usage code	Exclusivity Code	Exclusivity Date	Dosage	Strength	Product Number	Route	RLD	Pater Requ

No pharmaceuticals data

AA/SWA Ex. 1015, p.449 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Citations

Display in a list (/api/control?client=&citationsSearch=_)

AA/SWA Ex. 1015, p.450 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

☐	backward	US5159592A	By other than the examiner	1992-10-27	Network address management for a wired network supporting wireless communication to a plurality of mobile users	IBM	
☐	backward	US5361256A	By other than the examiner	1994-11-01	Inter-domain multicast routing	IBM	
☐	backward	US5563878A	By other than the examiner	1996-10-08	Transaction message routing in digital communication networks	IBM	
☐	backward	US5623605A	By other than the examiner	1997-04-22	Methods and systems for interprocess communication and inter-network data transfer	LUCENT TECHNOLOGIES	
☐	backward	US5701427A	By other than the examiner	1997-12-23	Information transfer arrangement for distributed computer system	DIGITAL EQUIPMENT	
☐	backward	US5717686A	By other than the examiner	1998-02-10	Cellular spacecraft TDMA communications system with call interrupt coding system for maximizing traffic throughput	LOCKHEED	
☐	backward	US5717687A	By other than the examiner	1998-02-10	Data communication system with adaptive routing, and switching node intended to be used in such a system	PHILIPS	
☐	backward	US5734651A	By other than the examiner	1998-03-31	Transaction message routing in digital communication networks	IBM	
☐	backward	US5751961A	By other than the examiner	1998-05-12	Integrated internet system for translating logical addresses of internet documents to physical addresses using integrated service control point	BELL COMMUNICATIONS RES	
☐	backward	US5754938A	Cited by the examiner	1998-05-19	Pseudonymous server for system for customized electronic identification of desirable objects	HERZ FREDERICK S. M EISNER JASON M SALGANICOFF MARCOS	
☐	backward	US5764906A	By other than the examiner	1998-06-09	Universal electronic resource denotation, request and delivery system	NETWORD	
☐	backward	US5777989A	By other than the examiner	1998-07-07	TCP/IP host name resolution for machines on several domains	IBM	
☐	backward	US5781550A	By other than the examiner	1998-07-14	Transparent and secure network gateway	DIGITAL EQUIPMENT	
☐	backward	US5790548A	By other than the examiner	1998-08-04	Universal access multimedia data network	BELL ATLANTIC NETWORK SERVICES	
☐	backward	US5793763A	By other than the examiner	1998-08-11	Security system for network address translation systems	CISCO TECH	
☐	backward	US5805818A	By other than the examiner	1998-09-08	System for acknowledging availability of neighbor node using data packet containing data that is ordinarily fowarded to neighbor node	NOVELL	
☐	backward	US5805820A	By other than the examiner	1998-09-08	Method and apparatus for restricting access to private information in domain	AT & T	

AA/SWA Ex. 1015, p.451 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

					name systems by redirecting query requests		
☐	backward	US5815664A	By other than the examiner	1998-09-29	Address reporting device and method for detecting authorized and unauthorized addresses in a network environment	FUJITSU	
☐	backward	US5826014A	By other than the examiner	1998-10-20	Firewall system for protecting network elements connected to a public network	NETWORK ENGINEERING SOFTWARE	
☐	backward	US5856974A	By other than the examiner	1999-01-05	Internetwork address mapping gateway	NOVELL	

1 - 20 of 280

Non-patent literature

Venters, Demystifying Protocols: A comparison of Protocols Suitable for IP Telephony, Sonus Networks, pp. 1-11, 2000.
Tsuchiya, et al., Extending the IP Internet Through Address Reuse, ACM SIGCOMM Computer Communication Review, pp. 16-33, Jan. 1993.
Francis, et al., IPNL: A NAT-Extended Internet Architecture, SIGCOMM'01, Aug. 27-31, 2001, pp. 69-79. (/intapi/scopus/0034775310) **16** Citations in Scopus
Yalagandula, et al., Transparent Mobility with Minimal Infrastructure, University of Texas at Austin, pp. 1-14, Jul. 2001.
Teraoka, et al., VIP: A Protocol Providing Host Mobility, Communications of the ACM, Aug. 1994/vol. 37, No. 8, pp. 67-75, 113. (/intapi/scopus/0028485173) **20** Citations in Scopus
Egevang, et al., The IP Network Address Translator (NAT), Network Working Group, RFC 1631, May 1994, pp. 1-10.
Chatel, Classical Versus Transparent IP Proxies, Network Working Group, RFC 1919, Mar. 1996, pp. 1-35.
Finseth, An Access Control Protocol, Sometimes Called TACACS, Network Working Group, Jul. 1993, pp. 1-18.
Computer Nelowrks. Third Edition, by Andrew S. Tanenbaum, 1996, pp. 643-670, 685-691.
Perkins, Mobile IP, IEEE Communications Magazine, May 1997, pp. 84-99.
"Non-Final Office Action", U.S. Appl. No. 10/233,288, (Dec. 21, 2009), 13 pages.
"Final Office Action", U.S. Appl. No. 10/403,518, (Feb. 2, 2010), 26 pages.
"Final Office Action", U.S. Appl. No. 10/403,829, (Feb. 23, 2010), 15 pages.
"Advisory Action", U.S. Appl. No. 10/403,829, (May 14, 2010), 2 pages.
"Non Final Office Action", U.S. Appl. No. 10/161,573, (May 26, 2009),39 pages.
"Non Final Office Action", U.S. Appl. No. 10/403,829, (Jun. 22, 2009),26 pages.
Francis, Gummadi "IPNL: A NAT-Extended Internet Architecture", SIGCOMM '01 , (Aug. 2001),69-79.
"Final Office Action", U.S. Appl. No. 10/161,573, (Jul. 23, 2010), 21 pages.
"Final Office Action", U.S. Appl. No. 10/233,288, (Aug. 3, 2010), 15 pages.
"Non Final Office Action", U.S. Appl. No. 10/403,518, (Aug. 3, 2010), 30 pages.
"Advisory Action", U.S. Appl. No. 10/233,288, (Oct. 15, 2010), 3 pages.
Tanenbaum, Andrew S., "Computer Networks", Third Edition,(1996),1-37.
Chatel, M "Classical versus Transparent IP Proxies", Network Working Group Request for Comments , (Mar. 1996),1-35.
Finseth, C "An Access Control Protocol , Sometimes Called TACACS", Network Working Group Request for Comments , (Jul. 1993),1-18.
Francis, Paul et al., "IPNL: A NAT-Extended Internet Architecture", SIGCOMM'01 , (Aug. 1, 2008),69-79.
Perkins, Charles E., "Mobile IP", IEEE Communications Magazine , Sun Microsystems,(May 1997),84-99.
Teraoka, Fumio et al., "VIP: A Protocol Providing Host Mobility", Communications of the ACM , vol. 37, No. 8,(Aug. 1994),67-75, 113. (/intapi/scopus/0028485173) **20** Citations in Scopus
Tsuchiya, Paul F., et al., "Extending the IP Internet Through Address Reuse", ACM SIGCOMM Computer Communication Review , (January 1993),16-33.
Venters, Tracy "Demystifying Protocols: A Comparison of Protocols Suitable for IP Telephony", Sonus Networks , (2000),1-11.
Yalagandula, Praveen et al., "Transparent Mobility with Minimal Infrastucture", University of Texas at Austin , (Jul. 2001),1-14.
Kessler, Gary C., "Mobile IP: Harbiner of Untethered Computing," http://www.garykessler,net/librarymobileip.htm, Jan. 20, 2004.
Rekhter, "Cisco Systems' Tag Switching Architecture overview," Network Working Group, Feb. 1997.
Kent, "Security Architecture for the Internet Protocol," Network Working Group, Nov. 1998.
Computer Dictionary; Microsoft Press; 3rd Edition; 1997; p. 264.
K. Egevang and P. Francis, RFC 1631, The IP Network Address Translator (NAT), May 1994.
"Non Final Office Action", U.S. Appl. No. 10/403,829, (Nov. 19, 2010),19 pages.

Similar documents

Display in a list (/api/control?client=&similarSearch=_)

The similarity check is done by matching this document to all documents in the database. Only the title and abstract text are matched, resulting in a score. The 10 highest-scoring documents are displayed here.

☐ All

☐ Secure virtual address realm

AA/SWA Ex. 1015, p.452 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Publication number US20040249974A1
Publication date 2004-12-09
Application date 2003-03-31

A private virtual dynamic network is provided for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. In one embodiment, the present invention provides a separate private virtual address realm, seen to each user as a private network, while seamlessly crossing public and private network boundaries. One implementation of the present invention uses an agent to enable an entity to participate in the network without requiring the member to add new hardware or software.

☐ Group agent

Publication number US20040249973A1
Publication date 2004-12-09
Application date 2003-03-31

A private virtual dynamic network is provided for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. In one embodiment, the present invention provides a separate private virtual address realm, seen to each user as a private network, while seamlessly crossing public and private network boundaries. One implementation of the present invention uses an agent to enable an entity to participate in the network without requiring the member to add new hardware or software.

☐ System And Method For A Virtual Mobile Network

Publication number US20060217112A1
Publication date 2006-09-28
Application date 2006-03-23

A system, various methods, and various apparatuses are provided whereby a virtual mobile network can be created, in which multiple disparate networks can be interconnected to form a unified network environment. In this virtual mobile network environment a user can roam and handover an active call seamlessly between any two interconnected networks. For example, between: a) two private networks, b) a private network and a public cellular network and c) a private network and a public carrier network. The system also enables a user to access enterprise communications services in one network from any networks within this virtual Mobile network environment seamlessly.

☐ PRIVATE VIRTUAL LAN SPANNING A PUBLIC NETWORK FOR CONNECTION OF ARBITRARY HOSTS

Publication number IN4257CHENP2009A
Publication date 2009-08-14
Application date 2009-07-17

Architecture for exposing a virtual private network of peer devices into the public domain via an overlay network. Computing devices, peripheral devices, as well as mobile devices can be physically distributed, but appear to belong to the same virtual private (or home) network, and be accessible from anywhere. Benefits include access to user media/documents from anywhere, searching of all connected devices from one location, multicast and broadcast connectivity, management of the private network and the associated policies, and device discovery on the private network from across public networks. P2P networks and ad-hoc networks can be exposed as a virtual interface, as well as the utilization of client operating systems to create the virtual network, grouping, graphing, the integration with relay services and other NAT/firewall traversal schemes, and the creation of a P2P overlay manager on a physical NIC (network interface card) address rather than a virtual address.

☐ Private virtual LAN spanning a public network for connection of arbitrary hosts

Publication number US8489701B2
Publication date 2013-07-16
Application date 2007-06-28

Architecture for exposing a virtual private network of peer devices into the public domain via an overlay network. Computing devices, peripheral devices, as well as mobile devices can be physically distributed, but appear to belong to the same virtual private (or home) network, and be accessible from anywhere. Benefits include access to user media/documents from anywhere, searching of all connected devices from one location, multicast and broadcast connectivity, management of the private network and the associated policies, and device discovery on the private network from across public networks. P2P networks and ad-hoc networks can be exposed as a virtual interface, as well as the utilization of client operating systems to create the virtual network, grouping, graphing, the integration with relay services and other NAT/firewall traversal schemes, and the creation of a P2P overlay manager on a physical NIC (network interface card) address rather than a virtual address.

☐ Private virtual LAN spanning a public network for connection of arbitrary hosts

AA/SWA Ex. 1015, p.453 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Publication number CN101595688B
Publication date 2014-03-26
Application date 2008-01-15

Architecture for exposing a virtual private network of peer devices into the public domain via an overlay network. Computing devices, peripheral devices, as well as mobile devices can be physically distributed, but appear to belong to the same virtual private (or home) network, and be accessible from anywhere. Benefits include access to user media/documents from anywhere, searching of all connected devices from one location, multicast and broadcast connectivity, management of the private network and the associated policies, and device discovery on the private network from across public networks. P2P networks and ad-hoc networks can be exposed as a virtual interface, as well as the utilization of client operating systems to create the virtual network, grouping, graphing, the integration with relay services and other NAT/firewall traversal schemes, and the creation of a P2P overlay manager on a physical NIC (network interface card) address rather than a virtual address.

☐ PRIVATE VIRTUAL LAN SPANNING A PUBLIC NETWORK FOR CONNECTION OF ARBITRARY HOSTS

Publication number EP2127224A1
Publication date 2009-12-02
Application date 2008-01-15

Architecture for exposing a virtual private network of peer devices into the public domain via an overlay network. Computing devices, peripheral devices, as well as mobile devices can be physically distributed, but appear to belong to the same virtual private (or home) network, and be accessible from anywhere. Benefits include access to user media/documents from anywhere, searching of all connected devices from one location, multicast and broadcast connectivity, management of the private network and the associated policies, and device discovery on the private network from across public networks. P2P networks and ad-hoc networks can be exposed as a virtual interface, as well as the utilization of client operating systems to create the virtual network, grouping, graphing, the integration with relay services and other NAT/firewall traversal schemes, and the creation of a P2P overlay manager on a physical NIC (network interface card) address rather than a virtual address.

☐ PRIVATE VIRTUAL LAN SPANNING A PUBLIC NETWORK FOR CONNECTION OF ARBITRARY HOSTS

Publication number EP2127224A4
Publication date 2015-07-01
Application date 2008-01-15

Architecture for exposing a virtual private network of peer devices into the public domain via an overlay network. Computing devices, peripheral devices, as well as mobile devices can be physically distributed, but appear to belong to the same virtual private (or home) network, and be accessible from anywhere. Benefits include access to user media/documents from anywhere, searching of all connected devices from one location, multicast and broadcast connectivity, management of the private network and the associated policies, and device discovery on the private network from across public networks. P2P networks and ad-hoc networks can be exposed as a virtual interface, as well as the utilization of client operating systems to create the virtual network, grouping, graphing, the integration with relay services and other NAT/firewall traversal schemes, and the creation of a P2P overlay manager on a physical NIC (network interface card) address rather than a virtual address.

☐ PRIVATE VIRTUAL LAN SPANNING A PUBLIC NETWORK FOR CONNECTION OF ARBITRARY HOSTS

Publication number EP2127224B1
Publication date 2019-12-18
Application date 2008-01-15

Architecture for exposing a virtual private network of peer devices into the public domain via an overlay network. Computing devices, peripheral devices, as well as mobile devices can be physically distributed, but appear to belong to the same virtual private (or home) network, and be accessible from anywhere. Benefits include access to user media/documents from anywhere, searching of all connected devices from one location, multicast and broadcast connectivity, management of the private network and the associated policies, and device discovery on the private network from across public networks. P2P networks and ad-hoc networks can be exposed as a virtual interface, as well as the utilization of client operating systems to create the virtual network, grouping, graphing, the integration with relay services and other NAT/firewall traversal schemes, and the creation of a P2P overlay manager on a physical NIC (network interface card) address rather than a virtual address.

☐ PRIVATE VIRTUAL LAN SPANNING A PUBLIC NETWORK FOR CONNECTION OF ARBITRARY HOSTS

Publication number US20080183853A1
Publication date 2008-07-31
Application date 2007-06-28

Architecture for exposing a virtual private network of peer devices into the public domain via an overlay network. Computing devices, peripheral devices, as well as mobile devices can be physically distributed, but appear to belong to the same virtual private (or home) network, and be accessible from anywhere. Benefits include access to user media/documents from anywhere, searching of all connected devices from one location, multicast and broadcast connectivity, management of the private network and the associated policies, and device discovery on the private network from across public networks. P2P networks and ad-hoc networks can be exposed as a virtual interface, as well as the utilization of client operating systems to create the virtual network, grouping, graphing, the integration with relay services and other NAT/firewall traversal schemes, and the creation of a P2P overlay manager on a physical NIC (network interface card) address rather than a virtual address.

1
1

AA/SWA Ex. 1015, p.454 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Results for: 7949785 or 7,949,785 Terms and Connectors

Cases 0

No documents found in Cases

Try the following:

- Review your results in the other categories.
- Modify your search (edit or remove some search terms or add synonyms).
- Check for spelling errors.
- Note: Some content may not be visible based on the restrictions of your subscription.

Copyright © 2024 LexisNexis.

Results for: 7949785 or 7,949,785 Terms and Connectors

News 0

Magazines & Journals

Clear

No documents found in News filtered by Magazines & Journals.

Try the following:

- Remove one or more filters: Magazines & Journals
- Review your results in the other categories.
- Modify your search (edit or remove some search terms or add synonyms).
- Check for spelling errors.

Copyright © 2024 LexisNexis.

User Name: Patricia Martin
Date and Time: Monday, June 3, 2024 4:07:00PM EDT
Job Number: 225731191

Documents (2)

1. *US Patent Issued to Inpro Network Facility on May 24 for "Secure Virtual Community Network System" (California Inventors)*
   Client/Matter: -None-
   Search Terms: 7949785 or 7,949,785
   Search Type: Terms and Connectors
   Narrowed by:

Content Type	Narrowed by
	-None-

2. *Inpro Network Facility Assigned Patent*
   Client/Matter: -None-
   Search Terms: 7949785 or 7,949,785
   Search Type: Terms and Connectors
   Narrowed by:

Content Type	Narrowed by
	-None-

LexisNexis | About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2024 LexisNexis

US Patent Issued to Inpro Network Facility on May 24 for "Secure Virtual Community Network System" (California Inventors)

US Fed News

May 30, 2011 Monday 9:39 AM EST

Copyright 2011 HT Media Ltd. All Rights Reserved

Length: 236 words

Dateline: ALEXANDRIA, Va.

Load-Date: May 30, 2011

End of Document

Body

ALEXANDRIA, Va., May 30 -- United States ***Patent*** no. ***7,949,785***, issued on May 24, was assigned to Inpro Network Facility LLC (Wilmington, Del.).

"Secure Virtual Community Network System" was invented by Hasan S. Alkhatib (Saratoga, Calif.), Fouad A. Tobagi (Los Altos, Calif.) and Farid F. Elwailly (San Jose, Calif.).

According to the abstract released by the U.S. ***Patent*** & Trademark Office: "A private virtual dynamic network is provided for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. In one embodiment, the present invention provides a separate private virtual address realm, seen to each user as a private network, while seamlessly crossing public and private network boundaries. One implementation of the present invention uses an agent to enable an entity to participate in the network without requiring the member to add new hardware or software."

The ***patent*** was filed on March 31, 2003, under Application No. 10/403,818.

For further information please visit: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=7949785&OS=7949785&RS=7949785

For any query with respect to this article or any other content requirement, please contact Editor at htsyndication@hindustantimes.com

Patricia Martin

Inpro Network Facility Assigned Patent

Targeted News Service

May 26, 2011 Thursday 12:34 AM EST

SR0526HP0526-554518

Copyright 2011 Targeted News Service LLC All Rights Reserved

Length: 251 words

Byline: Targeted News Service

Dateline: Alexandria, Va.

Load-Date: September 22, 2011

End of Document

Body

ALEXANDRIA, Va., May 26 -- Inpro Network Facility, Wilmington, Del., has been assigned a ***patent*** (***7,949,785***) developed by Hasan S. Alkhatib, Saratoga, Calif., Fouad A. Tobagi, Los Altos, Calif., and Farid F. Elwailly, San Jose, Calif., for a "secure virtual community network system."

The abstract of the ***patent*** published by the U.S. ***Patent*** and Trademark Office states: "A private virtual dynamic network is provided for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. In one embodiment, the present invention provides a separate private virtual address realm, seen to each user as a private network, while seamlessly crossing public and private network boundaries. One implementation of the present invention uses an agent to enable an entity to participate in the network without requiring the member to add new hardware or software."

The ***patent*** application was filed on March 31, 2003 (10/403,818). The full-text of the ***patent*** can be found at http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=7,949,785&OS=7,949,785&RS=7,949,785

Written by Satyaban Rath; edited by Hemanta Panigrahi.

For more information about Targeted News Service federal ***patent*** awards please contact: Myron Struck, Editor, Direct: 703/866-4708, Cell: 703/304-1897, Myron@largelednews.com

Patricia Martin

COPTO/SB/08a (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 contains a valid OMB control number.

Substitute for form 1449/PTO			***Complete if Known***	
			Application Number	In *Ex Parte* Reexamination of U.S. Patent 7,949,785
INFORMATION DISCLOSURE STATEMENT *(Use as many sheets as necessary)*			Filing Date	Herewith
			First Named Inventor	Hasan S. Alkhatib
			Art Unit	TBD
			Examiner Name	TBD
Sheet 1	of	2	Attorney Docket Number	IVI785

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.1	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	EX1005	7,036,143	04-25-2006	Leung et al.	
	EX1006	7,155,518	12-26-2006	Forslow et al.	
	EX1007	2003/0028671	02-06-2003	Mehta et al.	
	EX1008	7,290,060	10-30-2007	Kong	
	EX1009	7,533,164	05-12-2009	*Volz et al.*	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.1	Foreign Patent Document Country Code3 –Number 4 –Kind Code5 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T6

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

PTO/SB/08a (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 contains a valid OMB control number.

Substitute for form 1449/PTO				***Complete if Known***	
				Application Number	In *Ex Parte* Reexamination of U.S. Patent 7,949,785
INFORMATION DISCLOSURE STATEMENT *(Use as many sheets as necessary)*				Filing Date	Herewith
				First Named Inventor	Hasan S Alkhatib
				Art Unit	TBD
				Examiner Name	TBD
Sheet	2	of	2	Attorney Docket Number	IVI785

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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.	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	EX1002	U.S. File History of the '785 Patent ("File History")	
	EX1003	Declaration of Dr. Michael I. Shamos ("Shamos Decl.")	
	EX1004	Curriculum Vitae of Dr. Michael I. Shamos	
	EX1010	Infringement Claim Chart from *Intellectual Ventures I LLC et al v. Comerica Inc.*, Case No. 2:23-cv-00524, Dkt. 1, Ex. 9 (E.D. Tex. Nov. 15, 2023)	
	EXAA	Claim Chart for Intellectual Ventures I LLC '785 Patent	

Examiner Signature	/DENNIS G BONSHOCK/	Date Considered	06/11/2024

*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.
This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.*

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.G.B/

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 2698

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
90/019,519	05/22/2024 RULE	709	3992	IVI785

APPLICANTS

INVENTORS

7949785, Residence Not Provided;
Unified Patents, LLC, Residence Not Provided;
Intellectual Ventures i LLC (Patent Owner), Wilmington, DE;
Unified Patents LLC (3rd Pty Req.), Chevy Chase, MD;
Hasan S. Alkhatib, Saratoga, CA;
Fouad A. Tobagi, Los Altos, CA;
Farid F. Elwailly, San Jose, CA;

**** CONTINUING DATA ***************************

This application is a REX of 10/403,818 03/31/2003 PAT 7949785
*

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and Acknowledged /DENNIS G BONSHOCK/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
				90	6

ADDRESS

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661
UNITED STATES

TITLE

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
0.00	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
Unified Patents, LLC 4445 Willard Ave., Suite 600 Chevy Chase, MD 20815

LITIGATION REVIEW ☑	/DGB/ (examiner initials)	11 June 2024 (date)
Case Name		Director Initials
· 1:24cv344 Assurant, Inc. v. Intellectual Ventures I LLC et al., US District Court, Delaware (OPEN)		
· 2:23cv523, Intellectual Ventures I LLC et al. v. JP Morgan Chase Bank, US District Court, Eastern District Texas (OPEN)		
· 2:23cv524, Intellectual Ventures I LLC et al. v. Comerica Incorporated, US District Court, Eastern District Texas (OPEN)		
· 2:23cv525, Intellectual Ventures I LLC et al. v. Liberty Mutual Holding Company, US District Court, Eastern District Texas (OPEN)		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

AA/SWA Ex. 1015, p.463 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

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.
90/019,519	05/22/2024	7949785	IVI785	2698

23446 7590 06/14/2024
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/14/2024	PAPER

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Unified Patents, LLC
4445 Willard Ave., Suite 600
Chevy Chase, MD 20815

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/019,519* .

PATENT UNDER REEXAMINATION *7949785* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Order Granting Request For Ex Parte Reexamination	Control No. 90/019,519	Patent Under Reexamination 7949785	
	Examiner DENNIS G BONSHOCK	Art Unit 3992	AIA (FITF) Status No

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

The request for *ex parte* reexamination filed 05/22/2024 has been considered and a determination has been made. An identification of the claims, the references relied upon, and the rationale supporting the determination are attached.

Attachments: a)☐ PTO-892, b)☑ PTO/SB/08, c)☐ Other: ____

1. ☑ The request for *ex parte* reexamination is GRANTED.

RESPONSE TIMES ARE SET AS FOLLOWS:

For Patent Owner's Statement (Optional): TWO MONTHS from the mailing date of this communication (37 CFR 1.530 (b)). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**

For Requester's Reply (optional): TWO MONTHS from the **date of service** of any timely filed Patent Owner's Statement (37 CFR 1.535). **NO EXTENSION OF THIS TIME PERIOD IS PERMITTED.** If Patent Owner does not file a timely statement under 37 CFR 1.530(b), then no reply by requester is permitted.

/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	/JOSHUA D CAMPBELL/ Primary Examiner, Art Unit 3992	

cc:Requester (if third party requester)

Notice of Pre-AIA or AIA Status

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

DECISION ON REQUEST FOR REEXAMINATION

A substantial new question (SNQ) of patentability affecting claims 30 and 34 of United States Patent Number: 7,949,785 issued to Alkhatib et al. (hereinafter the '785 Patent) is raised by the Request for *ex parte* reexamination filed 5/22/2024.

The Office's determination in both the order for reexamination and the examination stage of the reexamination ordered will generally be limited solely to a review of the claim(s) for which reexamination was requested (see: MPEP 2240 & 2243). Additionally, if a Requester fails to set forth the pertinency and manner of applying the cited art to a claim as required by 37 CFR 1.510(b), that claim will generally not be reexamined. This matter was squarely addressed in *Sony Computer Entertainment America Inc. v. Dudas*, 85 USPQ2d 1594 (E.D. Va 2006). The District Court upheld the Office's discretion to not reexamine claims in an *Inter Partes* Reexamination proceeding other than those claims for which reexamination had specifically been requested.

Information Disclosure Statement

Regarding Information Disclosure Statement (IDS) submissions, MPEP 2256 recites the following: "Where patents, publications, and other such items of information are submitted by a party (patent owner or requester) in compliance with the requirements of the rules, the requisite degree of consideration to be given to such information will be normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information. The initials of the examiner placed adjacent to the citations on the form PTO/SB/08A and 08B or its equivalent, without an indication to the contrary in the record, do not signify that the information has been considered by the examiner any further than to the extent noted above."

Accordingly, the IDS submission filed by Third Party Requester (3PR) on 5/22/2024 has been considered by the Examiner only with the scope required by MPEP 2256, unless otherwise noted.

References

The Request presents that the following references raise an SNQ with regard to claims 30 and 34 of the '785 Patent:

- U.S. Patent No. 7,036,143 to Leung et al. (hereinafter Leung)
- U.S. Patent No. 7,155,518 to Forslöw et al. (hereinafter Forslöw)
- U.S. Publication No. 2003/0028671 to Mehta et al. (hereinafter Mehta)

Affidavits, Declaration, or Other Written Evidence

The Examiner recognizes that a declaration by Dr. Michael I. Shamos (executed on 5/22/2024) has been referenced in support of Third Party Requester. The declaration (hereafter the "Shamos Declaration") has been considered and made of record.

The Examiner further notes that affidavits or declarations or other written evidence which explain the contents or pertinent dates of prior art patents or printed publications in more detail may be considered in reexamination (see: MPEP 2258(I)(E)), but any rejection must be based upon the prior art patents or printed publications as explained by the affidavits or declarations or other written evidence. The rejection in such circumstances cannot be based on the affidavits or declarations or other written evidence as such, but must be based on the prior art patents or printed publications.

Prosecution History

Original Examination:

The 7,949,785 patent resulted from the 10/403,818 application which was filed on March 31, 2003.

On 9/22/2006, the Office issued a Non-Final Office action rejecting all claims under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application No. 2003/0041136 to Cheline et al.

On 3/22/2007, Patent Owner (then Applicant) filed a response with a series of amendments to the claims. Specifically, noting that the network traffic router "uses router data to route traffic between members of the virtual community" and that "a first member of the virtual community communicates with another member in the virtual community by querying the DNS server to determine a virtual network address and a private network address for the another member, and to determine a public address of the network traffic router."

On 6/5/2007, a Final Office action issued rejecting all claims either over Cheline alone or Cheline in view of US Patent Publication No. 2004/0006708 to Mukherjee.

On 12/4/2007, Patent Owner filed an RCE heavily amending the claim set

On 2/4/2009, the Office largely rejected most claims under 35 U.S.C. 101 as being directed toward "software elements". Then rejecting the amended claims under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application No.: 2008/0232295 by Kreiner et al. Examiner further noted that *"Claims 16 and 44 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims." See claim 16 below (claims 44 was similarly worded)*

16. (currently amended) The system of claim 1 wherein the virtual network manager is further configured to receive a DNS request from the source device, and return a public network address of the route director, a private network address for the destination device, and the second virtual network address that corresponds to the destination device, ~~claim 15 wherein said second device includes at least one private physical address.~~

On 9/1/2010, the Office issued an office action noting allowability of claims 1-15, 17-24, 26-36, 41-43, and 93-109, noting: *"the prior art was not found to teach or suggest returning a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device in response to a DNS request in the context of claims 1, 32, and 93. Specifically, no examples were found in the prior art of record in which both a private address and a virtual address of a destination device would be returned." The office action further rejected claims 53-66 and 68-92 under* 35 U.S.C. 102(e) as being anticipated by U.S. Patent No.: 6,631,416 to Bendinelli.

On 11/5/2010, the Office issued a non-final office action again returning to rejecting claims 1-15, 17-24, 26-36, 41-43, and 80-92 under 35 U.S.C. 101 as being broad enough to be directed toward "software per se".

On 12/2/2010, the Patent Owner filed claim amendments grounding the claims in hardware.

On 1/14/2011, the Office issued a Notice of Allowability giving no further reasons for allowance.

Litigation History

- 1:24cv344 Assurant, Inc. v. Intellectual Ventures I LLC et al., US District Court, Delaware (OPEN)
- 2:23cv523, Intellectual Ventures I LLC et al. v. JP Morgan Chase Bank, US District Court, Eastern District Texas (OPEN)
- 2:23cv524, Intellectual Ventures I LLC et al. v. Comerica Incorporated, US District Court, Eastern District Texas (OPEN)
- 2:23cv525, Intellectual Ventures I LLC et al. v. Liberty Mutual Holding Company, US District Court, Eastern District Texas (OPEN)

Substantial New Question of Patentability

The presence or absence of "a substantial new question of patentability" determines whether or not reexamination is ordered. For a substantial new question of patentability to be present, it is only necessary that: (A) the prior art patents and/or printed publications raise a substantial question of patentability regarding at least one claim, i.e., the teaching of the (prior art) patents and printed publications is such that a reasonable examiner would consider the teaching to be important in deciding whether or not the claim is patentable; and (B) the same question of patentability as to the claim has not been decided by the Office in an earlier concluded examination or review of the patent, raised to or by the Office in a pending reexamination or supplemental

examination of the patent, or decided in a final holding of invalidity (after all appeals) by a federal court in a decision on the merits involving the claim. If a reexamination proceeding was terminated/vacated without resolving the substantial question of patentability question, it can be re-presented in a new reexamination request. It is not necessary that a "prima facie" case of unpatentability exist as to the claim in order for a substantial new question of patentability to be present as to the claim. Thus, a substantial new question of patentability as to a patent claim could be present even if the examiner would not necessarily reject the claim as either fully anticipated by, or obvious in view of, the prior art patents or printed publications (see: MPEP 2242(I)).

In a decision to order reexamination made on or after November 2, 2002, reliance on old art does not necessarily preclude the existence of a substantial new question of patentability that is based exclusively on that old art. See Public Law 107-273, 116 Stat. 1758, 1899-1906 (2002), which expanded the scope of what qualifies for a substantial new question of patentability upon which a reexamination may be based. Determinations on whether a substantial new question of patentability exists in such an instance shall be based upon a fact-specific inquiry done on a case-by-case basis. For example, a substantial new question of patentability may be based solely on old art where the old art is being presented/viewed in a new light, or in a different way, as compared with its use in the earlier examination(s), in view of a material new argument or interpretation presented in the request. Such material new argument or interpretation may be based solely on claim scope of the patent being reexamined (see: MPEP 2242(II)(A)).

Claim 30 is presented below **bolded** in areas showing the limitations that are believed to be the critical limitations, given the prosecution history recited above, and which are used by the Examiner to show how specific teachings of the proposed references raise a substantial new question of patentability.

30. A virtual network manager, comprising:

a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;

a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to:

receive a registration request from an agent associated with a device;

distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and

a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device*.*

In the 5/22/2024 Request, the 3PR (Requester) suggests that the following combination of references provide elements which are allegedly equivalent to claims 30 and 34 of the '785 Patent.

Proposed Ground 1: Claims 30 and 34 over a Leung, Forslöw, and Mehta

---

The Requestor alleges that the combination of the Leung, Forslöw, and Mehta references raises a substantial new question of patentability with respect to claim 30 of the '785 patent. Reading of the Leung, Forslöw, and Mehta reference on the claims is provided on pages 13-22 of the Request and in Exhibit AA.

Both Leung and Mehta references is new art that provides new, non-cumulative technological teachings that were not previously considered nor discussed on the record during prosecution of the '785 patent. Though an earlier publication of Forslöw was cited in a 'Notice of References Cited', it was not specifically cited against the claims and in any case Forslöw is presented, in this reexamination, combined with the Leung and Mehta references.

With regard to the limitation of ***the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated***

with a second device in the virtual network, and a virtual network address associated with the second device, Leung teaches a virtual private network system (VPN) in which client devices gain access to the VPN in order to send data to devices within the VPN (see 5:8-18; Ex. 1003, 956-961). Leung is further supplemented by the teaching of Forslöw and Mehta:

Forslöw discloses a similar VPN, but specifically details the way in which the DNS server (which it calls a mobile service manager) facilitates communication over the VPN system, by receiving a request and returning a triplet, including a mobile node private IP address 156b (i.e., a private network address associated with a second device in the virtual network) and a virtual home agent's 1b public IP address 157b (i.e., a virtual network address associated with the second device). (see 9:62-10:20). Additionally, Forslöw's VPN system provides for a virtual route director (virtual router) to assist in data mapping. (see 9:19-29).

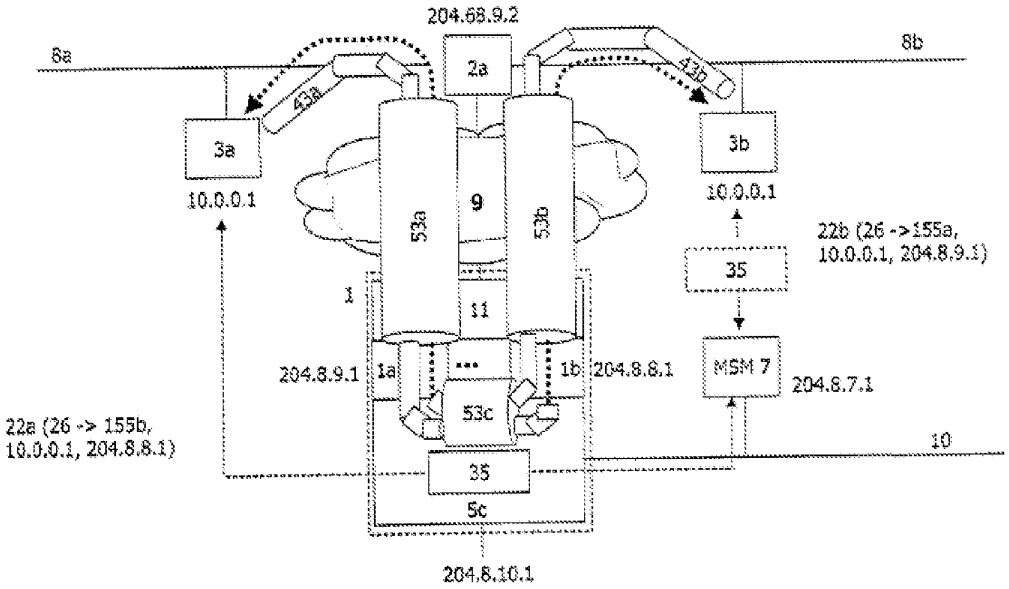
Specifically:

- Each virtual home agent has all the components of a physical home agent. A virtual router dispatcher 11 is placed in front of the virtual home agents 1a and 1b, in order to distribute datagrams internally in the home agent 1 based on destination IP addresses. (see 9:19-29)
- The home agent 1 also contains a backbone virtual router 5c that act as the common gateway towards the Internet 6 for all virtual home agents 1a and 1b. The backbone virtual home agent 5c also hosts a management network 10 to which a mobile service manager 7 for the mobile workgroup system is attached.

The mobile service manager 7 contains among other things a portal for workgroup membership list retrieval. The workgroup membership list is used in this invention to handle communication between workgroup members belonging to different address realms (mobile virtual private networks). (see 9:30-43)

- The mobile nodes 3a and 3b that are belonging to an extranet workgroup retrieve a list of workgroup members 26 by doing HTTPS requests 22a and 22b to the mobile service manager 7 and its portal. For each workgroup participant a triplet including the user fully qualified domain name 155b / 155a, the mobile node 3 private IP address 156 a/b (10.0.0.1) and the virtual home agent's 1a / 1b public IP address 157 a/b (204.8.9.1 and 204.8.8.1 respectively). The triplets are retrieved at sign-on to the extranet workgroup and can be updated regularly through a push or pull procedure from the mobile service manager 7 portal. A network address port translator 35 in the backbone virtual router 5c allows for the traversal of the HTTPS requests 22a and 22b form the mobile notes 3a and 3b to the mobile service manager 7. (see 10:7-20)
- The center module of a virtual home agent 1a/b is the virtual router 5 a/b. The virtual router is making next hop decisions for datagrams passing through the virtual home agent 1 a/b. (see 12:14-21)

Fig. 2



Mehta discloses a similar virtual networking system that operates with a DNS server and a route director, but it goes into more details about the operation of the route director, and thus provides for such DNS servers to provide private to network address associated with a network address proxy machine. (see paragraphs [0012], [0031]-[0032]). Here Mehta discloses, or at least renders obvious a DNS server for the virtual network (e.g., a DNS'/API server of the Address Management Proxy System), the DNS server configured to receive a DNS request from a first device in the virtual network (e.g., DNS'/API server receives a request from a device on a public network), and return a network address associated with a network route director (e.g., the DNS'/API server

returns the determined public network address of the associated Address Proxy /Router machine).

Specifically:

- the AMPS comprises one or more modified DNS/API servers, one or more Address Proxy/Routers, and Address Management Data Server, one or more Address Data Repositories, and optionally a load balancer. The AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device. And returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device. The public address is then usable by the device on the external public network to send data to the wireless device. The temporary public address is, for example, an address associated with one of the Address Proxy/Routers, which are connected to the external public network and have access to the private addresses on the private wireless network. (see paragraph [0012])

- In operation, when a wired device such as wired device 201, desires to send data to wireless device 240, the wired device needs first to determine a routable address location of the wireless device 240 on the public network 210. …The Address Management Proxy System 220 receives the query and determines and assigns a public (routable) address from a pool of addresses, which address can be used as a destination address for data packets targeted to wireless device 240. … Once the Address Management Proxy System 220 has returned a

routable address to wired device 201, the wired device 201 can send data to that address. (see paragraph [0031])

- The DNS'/API servers 302 are either individually connected to a public network 310 or are connected to the load balancer 301 which is in turn connected to public network 310. Similarly, each Address Proxy/Router 305 is also connected to the public network 310, via the routable (public) address to which data from the external network 310 is sent that is destined for the wireless devices. … Each Address Proxy/Router 305 also uses the Address Management Data Server 303 or equivalent to create and update a series of routing tables that are used to assign public addresses to wireless devices as needed and to update the various mappings between public addresses and the non-routable (private) addresses of the wireless devices. (see paragraph [0032])

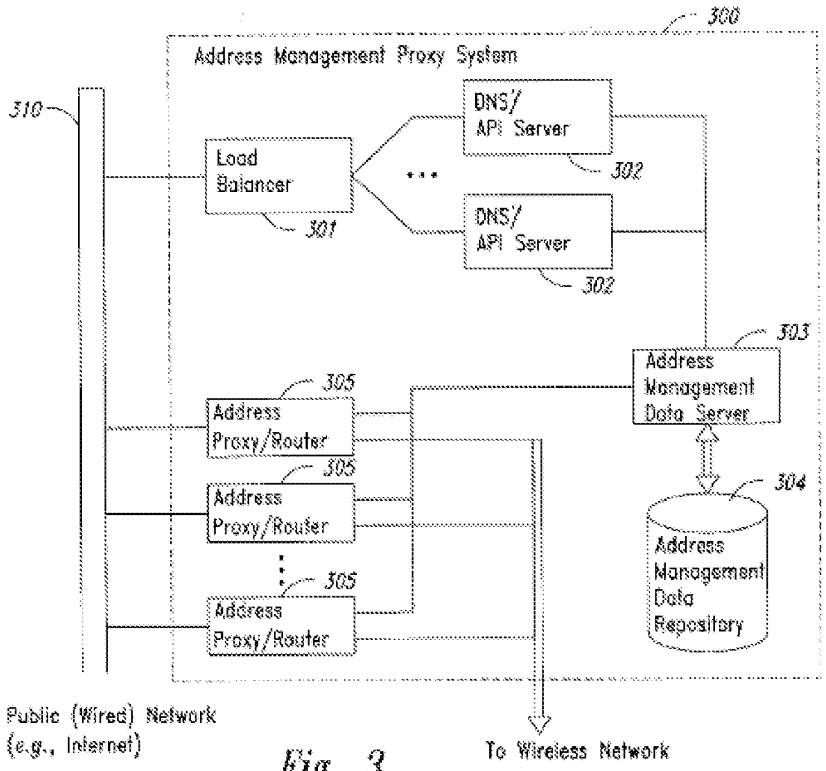


Fig. 3

It is agreed that the combination of the Leung, Forslöw, and Mehta references does raise a substantial new question of patentability, as proposed in the request, to at least claim 30 of the '785 patent. There is a substantial likelihood that a reasonable Examiner would consider these teachings important in deciding whether or not this claim is patentable.

Accordingly, the combination of the Leung, Forslöw, and Mehta references does raise a substantial new question to at least claim 30, which question has not been

decided in a previous examination of the '785 patent nor was there a final holding of invalidity by the Federal Courts regarding the '785 patent.

35 USC 325(d)

A review of the post grant history for the underlying patent indicates that there have been no other Office post grant challenges made to the patent (Reexamination Proceedings or *Inter Partes* Review, Post Grant Review, Covered Business Method trials). Accordingly, a discretionary denial of reexamination pursuant to 35 USC 325(d) is not applicable.

Summary

Claims 30 and 34 are hereby ORDERED to be reexamined.

Conclusion

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent throughout the course of this reexamination proceeding. The requester is also reminded of the ability to similarly appraise the Office

of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP § § 2207, 2282, and 2286.

All correspondence relating to this *ex parte* reexamination proceeding should be directed:

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

By FAX to: (571) 273-9900
Central Reexamination Unit

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

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/DENNIS G BONSHOCK/
Primary Examiner, Art Unit 3992

Conferees:
/JOSHUA D CAMPBELL/
Primary Examiner, Art Unit 3992

/ALEXANDER J KOSOWSKI/
Supervisory Patent Examiner, Art Unit 3992

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Previous Prosecution History	06/11/2024	DGB
Litigation History	06/11/2024	DGB
Patent Data Portal	06/11/2024	DGB
P-TACTS	06/11/2024	DGB

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

AA/SWA Ex. 1015, p.485 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 2698

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
90/019,519	05/22/2024 RULE	709	3992	IVI785

APPLICANTS

INTELLECTUAL VENTURES I, LLC. Organization, Residence Not Provided;

INVENTORS

7949785, Residence Not Provided;
Unified Patents, LLC, Residence Not Provided;
Intellectual Ventures i LLC (Patent Owner), Wilmington, DE;
Unified Patents LLC (3rd Pty Req.), Chevy Chase, MD;
Hasan S. Alkhatib, Saratoga, CA;
Fouad A. Tobagi, Los Altos, CA;
Farid F. Elwailly, San Jose, CA;

**** CONTINUING DATA ***************************

This application is a REX of 10/403,818 03/31/2003 PAT 7949785
*

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

Foreign Priority claimed ❑ Yes ❑ No 35 USC 119(a-d) conditions met ❑ Yes ❑ No Verified and Acknowledged _____ Examiner's Signature	❑ Met after Allowance _____ Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
				90	6

ADDRESS

VOLPE KOENIG
30 SOUTH 17TH STREET, 18TH FLOOR
PHILADELPHIA, PA 19103
UNITED STATES

TITLE

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

FILING FEE RECEIVED	FEES: Authority has been given in Paper	❑ All Fees
0.00	No._____ to charge/credit DEPOSIT ACCOUNT	❑ 1.16 Fees (Filing)
	No._____ for following:	❑ 1.17 Fees (Processing Ext. of time)
		❑ 1.18 Fees (Issue)
		❑ Other _____
		❑ Credit

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/019,519	**08/01/2024 04:29:49 PM Z ET**	**IVI785**

Title of Invention

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	7949785
CONFIRMATION #	2698	FILED BY	Margaret Ferello
PATENT CENTER #	66614700	FILING DATE	05/22/2024
CUSTOMER #	23446	FIRST NAMED INVENTOR	- 7949785
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brandon Theiss

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
IVIPR_RE90019519_Power_to_Prosecute_executed_pc.pdf	2	Power of Attorney	646 KB
Warning: The PDF file has been signed with a digital signature and the legal effect of the document will be based on the contents of the file not the digital signature.			
IVIPR_RE90019519_Statement_3_73_c_pc.pdf	3	Assignee showing of ownership per 37 CFR 3.73	590 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

IVIPR_RE90019519_Power_to_Prosecute_executed_pc.pdf	392AF667F7F6C6BEA7EF313B94A88763C0544E79413DED1B71DD7864E2E2354CEB097368800D423478738D89DD452ED44B3C065EBD7AD35EA6C3CFE7E13D0171
IVIPR_RE90019519_Statement_3_73_c_pc.pdf	4A1C9DCF3D1A9CCB71D6F3FF177327B1660AF5893E67F08A2D383E44D81A415957055A66DC808B9AAFB457316CE16372F701D1D2A3633C333AECA91823C72A43

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 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.

Docusign Envelope ID: 68133D08-EF23-472A-A3F2-7B6D18AF551C

PTO/AIA/80 (07-17)
Approved for use through 09/30/2025. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

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

I hereby appoint:

[X] Practitioners associated with Customer Number: 03624

OR

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

Name	Registration Number	Name	Registration Number

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

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

[X] The address associated with Customer Number: 03624

OR

[ ]

Firm or individual name Volpe Koenig		
Address		
City	State	Zip
Country		
Telephone	Email	

Assignee name and address: INTELLECTUAL VENTURES I LLC
3150 139th Avenue Southeast, Building 4
Bellevue, WA 98005

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

SIGNATURE of Assignee of Record

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

Signature MMacarthey (Docusigned by:)	Date 8/1/2024 | 12:49 PM EDT
Name Michelle Macarthey	Telephone
Title Assistant Company Secretary	

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0035. Public burden for this form is estimated to average 18 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.** If filing this completed form by mail, send to: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to: 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law; 2) a Federal, state, local, or international agency, in response to its request; 3) a contractor of the USPTO having need for the information in order to perform a contract; 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record; 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record; 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations; 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals; 8) 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)); 9) the Office of Personnel Management (OPM) for personnel research purposes; and 9) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Additional Uses

Additional USPTO uses of the information in this record may include disclosure to: 1) the International Bureau of the World Intellectual Property Organization, if the record is related to an international application filed under the Patent Cooperation Treaty; 2) the public i) after publication of the application pursuant to 35 U.S.C. 122(b), ii) after issuance of a patent pursuant to 35 U.S.C. 151, iii) if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections, or an issued patent, or iv) without publication of the application or patent under the specific circumstances provided for by 37 CFR 1.14(a)(1)(v)-(vii); and/or 3) the National Archives and Records Administration, for inspection of records.

PTO/AIA/96 (11-23)
Approved for use through 05/31/2024. 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.

STATEMENT UNDER 37 CFR 3.73(c)

First Named Inventor/Patent Owner: INTELLECTUAL VENTURES I LLC

Application No./Patent No.: RE 90/019,519 Filed/Issue Date: May 22, 2024

Titled: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

INTELLECTUAL VENTURES I LLC, a corporation

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

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

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

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

1. From: IP DYNAMICS INC. To: David Sun and Diana Sun

   The document was recorded in the United States Patent and Trademark Office at Reel 014196, Frame 0265, or for which a copy thereof is attached*.

2. From: Hasan S. Alkhatib, Fouad A.Tobagi; Farid E. Elwailly To: IP DYNAMICS INC.

   The document was recorded in the United States Patent and Trademark Office at Reel 014340, Frame 0968, or for which a copy thereof is attached*.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. 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.

PTO/AIA/96 (11-23)
Approved for use through 05/31/2024. 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.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: IP DYNAMICS INC. To: INPRO NETWORK FACILITY, LLC

The document was recorded in the United States Patent and Trademark Office at
Reel 020393, Frame 0423, or for which a copy thereof is attached*.

4. From: INPRO NETWORK FACILITY, LLC To: F. POSZAT H.U. LLC

The document was recorded in the United States Patent and Trademark Office at
Reel 037490, Frame 0592, or for which a copy thereof is attached*.

5. From: F. POSZAT HU, LLC To: INTELLECTUAL VENTURES I LLC

The document was recorded in the United States Patent and Trademark Office at
Reel 065469, Frame 0182, or for which a copy thereof is attached*.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached*.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

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

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

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Brandon R. Theiss	August 1, 2024
Signature	Date
/Brandon R. Theiss/	70,507
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to:

1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;

2) a federal, state, local, or international agency, in response to its request;

3) a contractor of the USPTO having need for the information in order to perform a contract;

4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;

5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;

6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;

7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;

8) 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));

9) the Office of Personnel Management (OPM) for personnel research purposes; and

10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
90/019,519	05/22/2024	7949785	IVI785

CONFIRMATION NO. 2698

3624
VOLPE KOENIG
30 SOUTH 17TH STREET, 18TH FLOOR
PHILADELPHIA, PA 19103

POA ACCEPTANCE LETTER

DC00000007602141 1

Date Mailed: 08/02/2024

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/01/2024.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/rbell/

AA/SWA Ex. 1015, p.494 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
90/019,519	05/22/2024	7949785	IVI785

CONFIRMATION NO. 2698

POWER OF ATTORNEY NOTICE

23446
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

Date Mailed: 08/02/2024

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/01/2024.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/rbell/

AA/SWA Ex. 1015, p.495 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
Unified Patents, LLC 4445 Willard Ave., Suite 600 Chevy Chase, MD 20815

LITIGATION REVIEW ☑	/DGB/ (examiner initials)	11 June 2024 (date)
Case Name		Director Initials
· 1:24cv344 Assurant, Inc. v. Intellectual Ventures I LLC et al., US District Court, Delaware (OPEN)		
· 2:23cv523, Intellectual Ventures I LLC et al. v. JP Morgan Chase Bank, US District Court, Eastern District Texas (OPEN)		
· 2:23cv524, Intellectual Ventures I LLC et al. v. Comerica Incorporated, US District Court, Eastern District Texas (OPEN)		
· 2:23cv525, Intellectual Ventures I LLC et al. v. Liberty Mutual Holding Company, US District Court, Eastern District Texas (OPEN)		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

AA/SWA Ex. 1015, p.496 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

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.
90/019,519	05/22/2024	7949785	IVIPR-RE90019519	2698

3624 7590 10/08/2024

VOLPE KOENIG
30 SOUTH 17TH STREET, 18TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
10/08/2024	PAPER

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Unified Patents, LLC
4445 Willard Ave., Suite 600
Chevy Chase, MD 20815

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/019,519* .

PATENT UNDER REEXAMINATION *7949785* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Office Action in Ex Parte Reexamination	**Control No.** 90/019,519	**Patent Under Reexamination** 7949785	
	Examiner DENNIS G BONSHOCK	**Art Unit** 3992	**AIA (FITF) Status** No

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

a. ☑ Responsive to the communication(s) filed on 22 May 2024.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

c. ☑ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter.
Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**
If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 30 and 34 are subject to reexamination.
1b. ☑ Claims 1-29,31-33 and 35-90 are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☐ Claims _____ are patentable and/or confirmed.
4. ☑ Claims 30 and 34 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
   1 ☐ been received.
   2 ☐ not been received.
   3 ☐ been filed in Application No. _____.
   4 ☐ been filed in reexamination Control No. _____.
   5 ☐ been received by the International Bureau in PCT application No. _____.
   * See the attached detailed Office action for a list of the certified copies not received.
9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

AA/SWA Ex. 1015, p.499 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Notice of Pre-AIA or AIA Status

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

Non-Final Office Action

This is a Non-Final action of claims 30 and 34 of United States Patent Number: 7,949,785 issued to Alkhatib et al. (hereinafter the '785 Patent). Reexamination was ordered on 6/14/2024 responsive to the Request for *ex parte* reexamination filed 5/22/2024. Responsive to the Office ordering reexamination, the Patent Owner chose not to file a Patent Owner statement.

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that *ex parte* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

References

- U.S. Patent No. 7,036,143 to Leung et al. (hereinafter Leung)
- U.S. Patent No. 7,155,518 to Forslöw et al. (hereinafter Forslöw)
- U.S. Publication No. 2003/0028671 to Mehta et al. (hereinafter Mehta)

Affidavits, Declaration, or Other Written Evidence

The Examiner recognizes that a declaration by Dr. Michael I. Shamos (executed on 5/22/2024) has been referenced in support of Third Party Requester. The declaration (hereafter the "Shamos Declaration") has been considered and made of record.

The Examiner further notes that affidavits or declarations or other written evidence which explain the contents or pertinent dates of prior art patents or printed publications in more detail may be considered in reexamination (see: MPEP 2258(I)(E)), but any rejection must be based upon the prior art patents or printed publications as explained by the affidavits or declarations or other written evidence. The rejection in such circumstances cannot be based on the affidavits or declarations or other written evidence as such, but must be based on the prior art patents or printed publications.

Prosecution History

Original Examination:

The 7,949,785 patent resulted from the 10/403,818 application which was filed on March 31, 2003.

On 9/22/2006, the Office issued a Non-Final Office action rejecting all claims under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application No. 2003/0041136 to Cheline et al.

On 3/22/2007, Patent Owner (then Applicant) filed a response with a series of amendments to the claims. Specifically, noting that the network traffic router "uses router data to route traffic between members of the virtual community" and that "a first member of the virtual community communicates with another member in the virtual community by querying the DNS server to determine a virtual network address and a private network address for the another member, and to determine a public address of the network traffic router."

On 6/5/2007, a Final Office action issued rejecting all claims either over Cheline alone or Cheline in view of US Patent Publication No. 2004/0006708 to Mukherjee.

On 12/4/2007, Patent Owner filed an RCE heavily amending the claim set

On 2/4/2009, the Office largely rejected most claims under 35 U.S.C. 101 as being directed toward "software elements". Then rejecting the amended claims under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application No.: 2008/0232295 by Kreiner et al. Examiner further noted that *"Claims 16 and 44 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims." See claim 16 below (claims 44 was similarly worded)*

> **16. (currently amended)** The system of claim 1 wherein the virtual network manager is further configured to receive a DNS request from the source device, and return a public network address of the route director, a private network address for the destination device, and the second virtual network address that corresponds to the destination device, ~~claim 15 wherein said second device includes at least one private physical address.~~

On 9/1/2010, the Office issued an office action noting allowability of claims 1-15, 17-24, 26-36, 41-43, and 93-109, noting: *"the prior art was not found to teach or suggest returning a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device in response to a DNS request in the context of claims 1, 32, and 93. Specifically, no examples were found in the prior art of record in which both a private address and a virtual address of a destination device would be returned." The office action further rejected claims 53-66 and 68-92 under* 35 U.S.C. 102(e) as being anticipated by U.S. Patent No.: 6,631,416 to Bendinelli.

On 11/5/2010, the Office issued a non-final office action again returning to rejecting claims 1-15, 17-24, 26-36, 41-43, and 80-92 under 35 U.S.C. 101 as being broad enough to be directed toward "software per se".

On 12/2/2010, the Patent Owner filed claim amendments grounding the claims in hardware.

On 1/14/2011, the Office issued a Notice of Allowability giving no further reasons for allowance.

Litigation History

- 1:24cv344 Assurant, Inc. v. Intellectual Ventures I LLC et al., US District Court, Delaware (OPEN)
- 2:23cv523, Intellectual Ventures I LLC et al. v. JP Morgan Chase Bank, US District Court, Eastern District Texas (OPEN)
- 2:23cv524, Intellectual Ventures I LLC et al. v. Comerica Incorporated, US District Court, Eastern District Texas (OPEN)
- 2:23cv525, Intellectual Ventures I LLC et al. v. Liberty Mutual Holding Company, US District Court, Eastern District Texas (OPEN)

Claim Rejections

Rejection 1 – as proposed in Grounds 1 – Leung, U.S. Patent No.: 7,036,143 (Ex. 1005) in view of Forslöw U.S. Patent No.: 7,155,518 (Ex. 1006) and Mehta U.S. Publication No.: 2003/0028671 (Ex. 1007) (see Request pages 13-22)

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any

correction of the statutory basis (i.e., changing from AIA to pre-AIA) for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

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

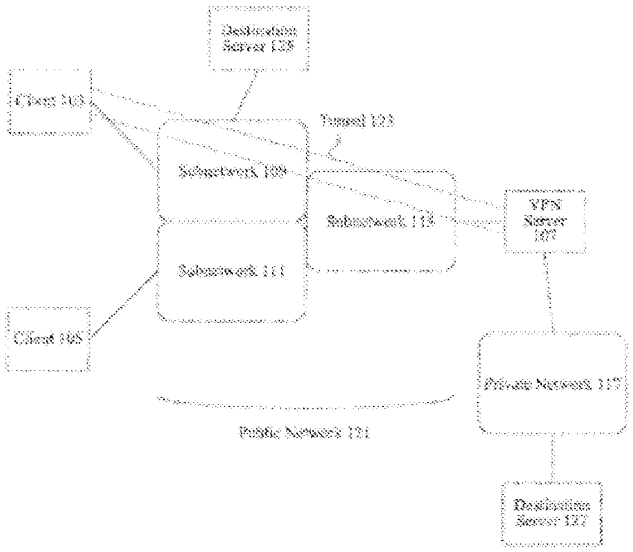
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention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

Claims 30 and 34 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Leung (U.S. Patent No. 7,036,143) in view of Forslöw (U.S. Patent No. 7,155,518) and Mehta (U.S. Publication No. 2003/0028671). Note: further rational for the combination can be found in Shamos Decl. ¶¶ 47-61.

With regard to claim 30, which teaches [30.0] "***A virtual network manager, comprising:***", Leung discloses a virtual network manager (e.g., a VPN server).

- FIG. 1 is a diagrammatic representation of a system in which embodiments of the present invention may be implemented. The subnetworks 109, 111, and 115 are part of a public network 121. The public network 121 can be connected with a variety of private networks as well as other public networks through different network nodes. For example, the public network 121 is connected to private network 117 through a VPN server 107. [4:57-64]

Figure 1



With regard to claim 30, which teaches [30.1] "***a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;***" Leung discloses a network interface (e.g., interfaces 1068) configured for data communication (e.g., control the sending and receiving of data products over the network) via a virtual network (e.g., a public network) that is defined by a domain name having an associated public network address (e.g., a subnetwork address from the Internet service provider associated with the subnetwork).

- Conventional virtual private networks deployed on a public network infrastructure provide clients the same security, management, quality of service policies, and benefits provided to clients in private networks. [1:12-15]

- The present invention may be implemented on a general-purpose network host machine such as a personal computer or workstation. Further, the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general purpose computing device. [11:12-17]

- The interfaces 1068 are typically provided as interface cards (sometimes referred to as “line cards”). Generally, they control the sending and receiving of data packets over the network and sometimes support other peripherals used with the router 1010. Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided such as fast Ethernet interfaces, Gigabit Ether net interfaces, ATM interfaces, HSSI interfaces, POS inter faces, FDDI interfaces and the like. Generally, these inter faces may include ports appropriate for communication with the appropriate media. [11:39-51]

- FIG. 10 is a diagrammatic representation of a general purpose computing device that can be used. The computing system 1010 suitable for implementing the present invention includes a master central processing unit (CPU) 1062, interfaces 1068, and a bus 1015 (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU 1062 is responsible for tasks such

as acquiring a subnetwork address or assigning an address to a TCP/IP stack. [11:20-28]

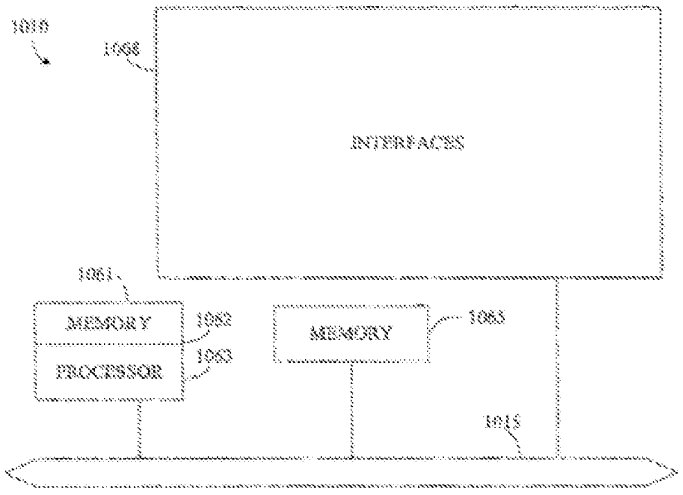


Figure 10

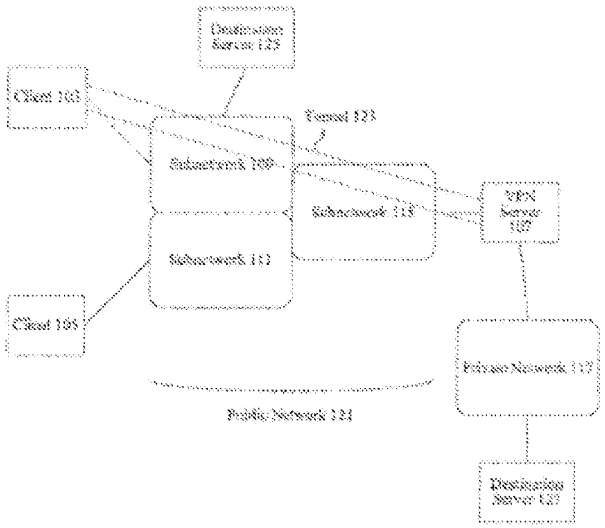
- The subnetworks 109, 111, and 115 are part of a public network 121. [4:59-60]

- The public network 121 is also connected to a destination server 125 as well as clients 103 and 105. In one example, a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 107. For instance, client 103 may be connected to public network 121 through an Internet service provider. In this example, client 103 may acquire a subnet work address from the Internet service provider associated with subnetwork 109. When the subnetwork address is obtained, the subnetwork address may be specifically associated with subnetwork 109. Using the

subnetwork address, client 103 can access a destination server 125 in a public network 121. [4:66-5:11]

- FIG. 1 is a diagrammatic representation of a system in which embodiments of the present invention may be implemented. The subnetworks 109, 111, and 115 are part of a public network 121. The public network 121 can be connected with a variety of private networks as well as other public networks through different network nodes. For example, the public network 121 is connected to private network 117 through a VPN server 107. [4:57-64]

Figure 1



A POSITA would have understood that the subnetwork address obtained from the Internet service provider disclosed in Leung is based on the domain name of the public network.

With regard to claim 30, which teaches [30.2] "***a memory and a processor to implement a register module configured to register devices in a virtual network, the register module further configured to:***", Leung discloses a memory (e.g., memory 1061) and a processor (e.g., CPU 1062) to implement a register module configured to register devices in a virtual network, (e.g., may be responsible for maintaining associations between clients and enterprises).

- A VPN client or a VPN server can be implemented on a general purpose computing device. FIG. 10 is a diagrammatic representation of a general purpose computing device that can be used. The computing system 1010 suitable for implementing the present invention includes a master central processing unit (CPU) 1062, interfaces 1068, and a bus 1015 (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU 1062 is responsible for tasks such as acquiring a subnetwork address or assigning an address to a TCP/IP stack. On the VPN server side, the CPU 1062 may be responsible for maintaining associations between clients and enterprises. The CPU 1062 may be a general purpose processor or it may be specially designed hardware for implementing a VPN client or a VPN server. In a specific embodiment, a memory 1061 (such as non-volatile RAM and/or ROM) also forms part of CPU 1062. However, there are many different ways in which memory could be coupled to the system. Memory block 1061 may be used for a variety of purposes such as, for example, caching and/or storing data, programming instructions, etc. [11:19-37]

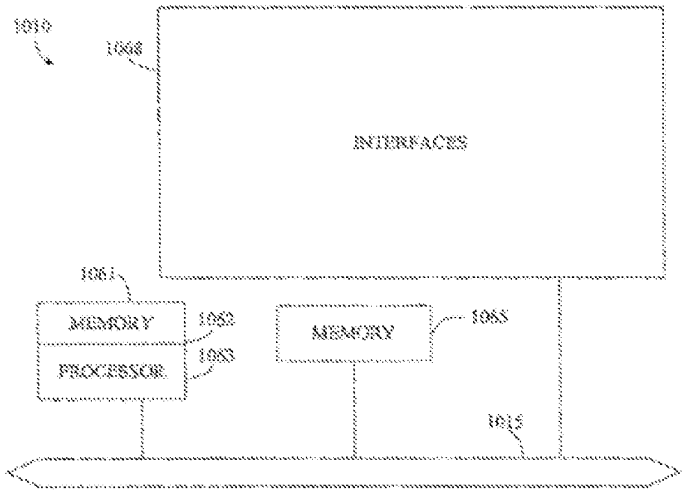


Figure 10

- The public network 121 is also connected to a destination server 125 as well as clients 103 and 105. In one example, a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 107. For instance, client 103 may be connected to public network 121 through an Internet service provider. In this example, client 103 may acquire a subnet work address from the Internet service provider associated with subnetwork 109. When the subnetwork address is obtained, the subnetwork address may be specifically associated with subnetwork 109. Using the subnetwork address, client 103 can access a destination server 125 in a public network 121. [4:66-5:11]

- When the subnetwork address is obtained, the subnetwork address may be specifically associated with subnetwork 109. Using the subnetwork address, client 103 can access a destination server 125 in a public network 121. However,

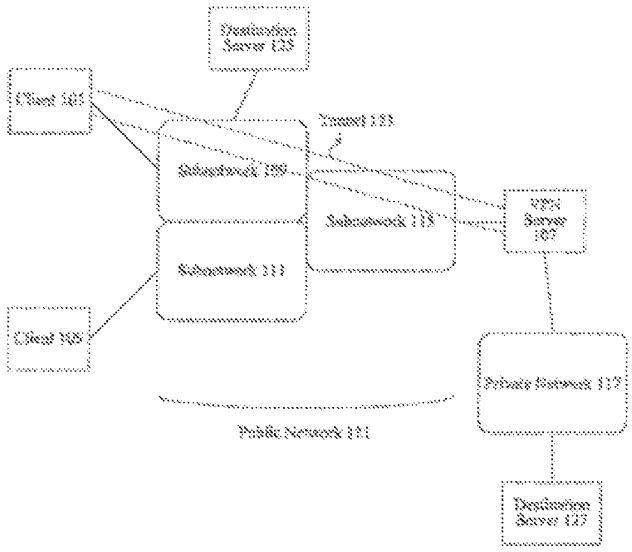
client 103 cannot access a private network destination server 127 until it is granted access by VPN server 107. To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107. [5:8-16]

With regard to claim 30, which teaches [30.2a] "***receive a registration request from an agent associated with a device;***" Leung discloses receive a registration request from an agent associated with a device (e.g., the VPN server receives a request for access from a VPN client).

- However, client 103 cannot access a private network destination server 127 until it is granted access by VPN server 107. To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107. In the access request, the client 103 provides information such as its subnetwork address, its user name, and its password. [5:11-18]

- In one example, a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 107. [4:67-5:33]

Figure 1



A POSITA would have understood that Leung's VPN clients would send registration requests via an associated agent. The '785 Patent describes "communication agent[s] installed on a device" that can include "software or hardware" and "may comprise a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address." Ex. 1001 at 7:1-8. Similarly, a POSITA would have understood Leung's VPN clients to include software to allow for traffic to be routed to members of the virtual community. This software would have been required for such a client device to send an access request to the VPN server. Thus, a POSITA would have understood that Leung discloses an agent associated with a device.

With regard to claim 30, which teaches [30.2b] "***distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address;***" Leung discloses distribute a virtual network address (e.g., enterprise address) to the device (e.g., VPN client) when the device is registered in the virtual network (e.g. private network), the device being identified to other devices in the virtual network by the virtual network address (e.g. the enterprise address allows the VPN server to identify a client).

- The client may therefore use the client subnetwork address to contact the VPN server and provide the VPN server with a user name and password to acquire an enterprise address. The enterprise address is the address that the VPN client uses to communicate with other nodes such as nodes in the company private network. [4:5-10]

- For instance, the enterprise address can be a company IP address. Thus, other nodes including nodes in the company private network will see the VPN client as having the enterprise address, and will therefore communicate with the VPN client via the enterprise address. Accordingly, sessions between the VPN client and a node of the private network can be conducted using the enterprise address. It should be noted that a client can have two distinct addresses. An address specific to a particular subnetwork that can be obtained from an ISP is referred to herein as a subnetwork address or a client subnetwork address. The subnetwork address can be an IP address. An address provided by a VPN server

and assigned to the client is referred to herein as an enterprise address. [4:12-25]

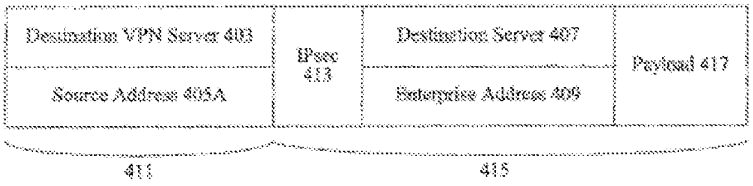
- To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107. In the access request, the client 103 provides information such as its subnetwork address, its user name, and its password. The VPN server 107 verifies the user name and password information from client 103 and provides the client 103 with an enterprise address. The enterprise address can be any address that allows a VPN server to identify a client 103. According to various embodiments, the enterprise address is a subnetwork address associated with the private network 117. For instance, the enterprise address may be a company IP address. [5:13-26]

- In this example, the encapsulated portion 415, however, is typically encrypted using IPsec 413. Encapsulated portion 415 provides the VPN tunnel with security. More particularly, security is provided through enabling authentication of the sender (e.g., via information in the encapsulated portion 415) and encryption of data as well. For instance, the encapsulated portion 415 preferably contains the enterprise address 409 allocated by the VPN server to the VPN client during the creation of the VPN tunnel, which may be used to authenticate the sender. The encapsulated portion 415 also contains the destination address of the server 407 that the client wishes to access. In one example, the destination server 407

may be a Web server containing a page that the client wishes to view. The encapsulated portion 415 may also contain a payload 417. [6:53-67]

- FIG. 4A is a diagrammatic representation of a message that can be sent from a client to a destination when a VPN tunnel is used. [6:41-43]

Figure 4A



- In one implementation, a client wishes to access a Web server. A client examines the access list to determine if the Web server address is on the access list. If the Web server address is not on the access list, the client can send a packet directly to the Web server using its subnetwork address as the source address and the address of the Web server as the destination address, as shown above. If the Web server is on the access list, the client is directed to send a packet to the Web server through a VPN tunnel and a VPN server. The client uses its own address as the source address and the address of the VPN server as the destination address of a message. The message contains an encapsulated portion 415 with a destination address 407 set as the address of the Web server and the source address 409 set as the enterprise address allocated by the VPN server. When the VPN server receives the message, the

VPN server can decrypt the message, authenticate the sender via the enterprise address (source address 409) and forward the encapsulated portion 415 of the message to the web server. [7:20-30]

- The web server receives the encapsulated portion of the message and sees that the source of the message is the enterprise address. The web server can send content to the enterprise address represented by the VPN server. The VPN server can then encapsulate the content and forward the content to the client. As noted above, the web server does not know the actual subnetwork address of the client. The web server may only know the enterprise address. In other words, the VPN server performs a mapping of the enterprise address to the client address. [7:20-30]

- The present invention allows the maintenance of existing sessions between a client and a destination node when the client moves from a first subnetwork to a second subnetwork. According to various embodiments, existing sessions can be maintained by modifying the VPN client and the VPN server. More particularly, the VPN client and the VPN server can be modified to allow the VPN client to use the same enterprise address whether the VPN client is in a first subnetwork or a second subnetwork. By using the same enterprise address, a client's existing sessions with a Web server, for example, can be maintained because the Web server can continue to send messages to the client using the same address. [8:1-13]

- FIG. 5 is a process flow diagram depicting some of the changes that can be made to the VPN client to allow the VPN client to seamlessly roam from a first subnetwork to a second subnetwork. At 501, a client is in a first subnetwork and obtains a first subnetwork address from an Internet service provider. The first subnetwork address is inserted into the TCP/IP stack to allow communication with other nodes in the network. At 505, the client attempts to set up a VPN tunnel with the VPN server by transmitting the first subnetwork address, a username, and a password to the VPN server. The VPN server verifies the information and provides the client with an enterprise address as well as an access list at 507. At 509, the client saves the first subnetwork address to use as an outer portion source address for outgoing packets. For instance, the first subnetwork address can be saved in the device driver or in the operating system. At 513, the VPN client replaces the first subnetwork address in the TCP/IP stack with the enterprise address acquired from the VPN server. By replacing the first subnetwork address with the enterprise address, the enterprise address can be used for all communications whether the client is in a first subnetwork or a second subnetwork. At 515, the client can send messages with or without the VPN tunnel. If messages are sent without the VPN tunnel, the source address is the first subnetwork address and the destination address can be the destination node of interest. If messages are sent through the VPN tunnel, the source address is the first subnetwork address and the destination address is the address of the VPN server. The encapsulated destination address is the destination node of interest and the encapsulated Source address is the

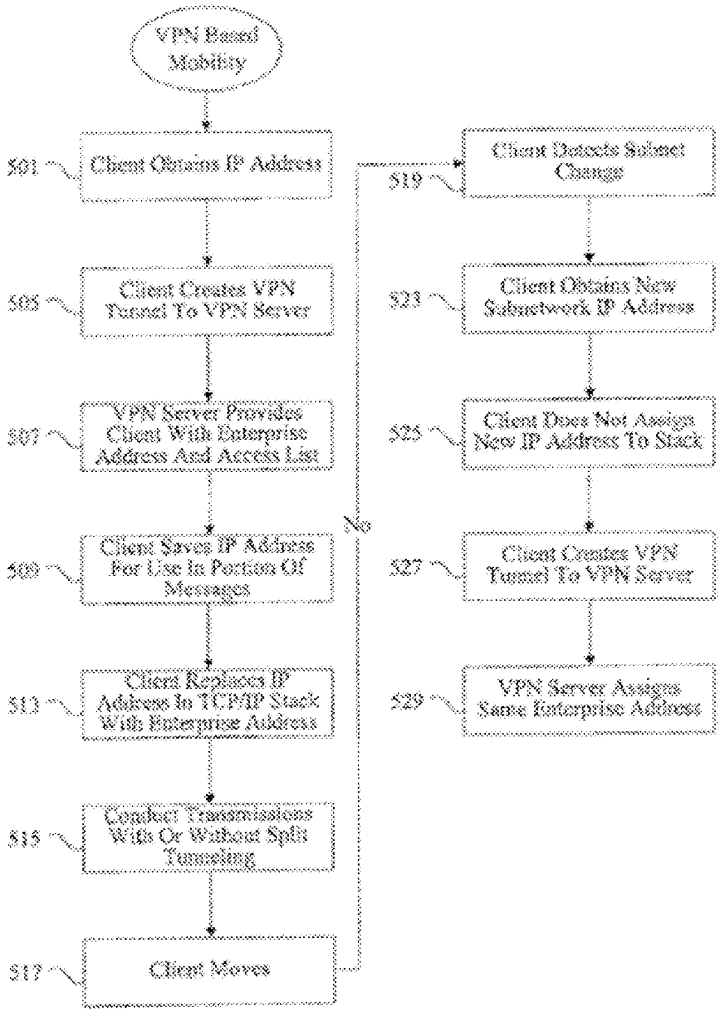
enterprise address. Such a message resembles the message shown in FIG. 4A. [8:14-45]

- At 517, the client moves from a first subnetwork to a second subnetwork. At 519, the client detects the change in subnetworks without user intervention. One of the benefits of the techniques of the present invention is that VPN based mobility can be accomplished in a manner transparent to the user. In many conventional applications, the client moving from a first subnetwork to a second subnetwork had to acquire a new subnetwork address and manually start the creation of anew VPN tunnel. Existing sessions would be dropped. However, the techniques of the present invention allow a VPN tunnel and existing sessions to be maintained without user interaction. The seamless mobility can be accomplished by automatically detecting a change in sub network using lower layer protocols. A variety of conventional mechanisms for detecting Subnet changes are available. Some techniques include using the lifetime field from a router advertisement using IRDP as described in RFC 1256 or using network prefixes as described in RFC 2002, the entirety of which is incorporated by references for all purposes. [8:46-65]

- The VPN client can then automatically obtain a second subnetwork address associated with the second subnetwork at 523. In one embodiment, the second subnetwork address can be obtained using DHCP. In other embodiments, a second subnetwork address can be automatically entered by a VPN client. At 525, the VPN client recognizes the change in Subnetworks and does not replace

the enterprise address in the TCP/IP stack with the second subnetwork address. The second subnetwork address instead can be saved in the device driver. The enterprise address remains the same in the TCP/IP stack. Without user intervention. the VPN client automatically attempts to re-establish the VPN tunnel by sending the second Subnetwork address, a username, and a password to the VPN server. The tunnel to the VPN server is created at 527. Because of modifications to the VPN server which will be discussed below, the VPN server assigns the same enterprise address to the VPN client at 529. By providing the same enterprise address to the VPN client, existing sessions are maintained. As will be appreciated by one of skill in the art, although the techniques of the present invention can be accomplished without user intervention, it will be appreciated that certain circumstances may benefit from user input. Various techniques for acquiring a new subnetwork address and establishing a VPN tunnel can also be accomplished manually. [8:66-9:23]

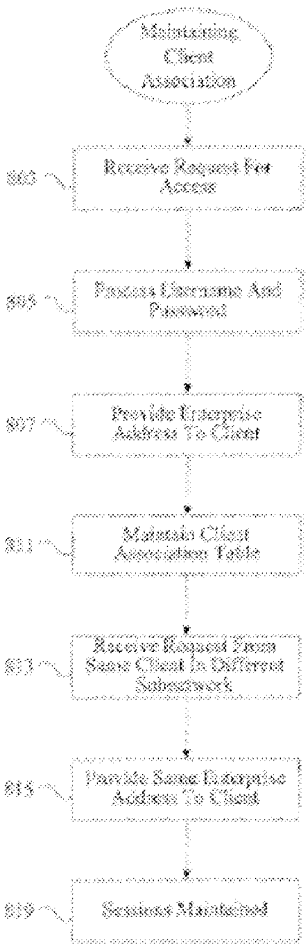
Figure 5



- FIG. 8 is a process flow diagram showing modifications to the server that can be used to provide a VPN client with the same enterprise address. At 803, the VPN server receives a request for access. The request for access may include the subnetwork address, a username, and a password of a VPN client. At 805, the VPN server verifies the username and password. At 807, the VPN server

provides an enterprise address to the VPN client to allow the VPN client to establish a VPN tunnel. The VPN server maintains a client association table at 811. Any mechanism providing an association between the client and the enterprise address is referred to herein as a client association table. For instance, the client association table can be maintained in a table listing usernames and their associated enterprise addresses. The client association table can also be maintained using various databases and log files providing information on client identifiers, usernames, and enterprise addresses. By maintaining an association between the client and the enterprise address, the VPN server can provide the same enterprise address to a client even if the client is registering from a different subnetwork address associated with a different subnetwork. If a client moves from a first subnetwork to a second subnetwork and registers with a second subnetwork address, the VPN server can recognize the client with the username. At 813, the VPN server receives an access request having a second Subnet work address, a username, and a password of the same VPN client. The VPN server can access the client association table to determine whether the VPN client has been provided an enterprise address in the past. The VPN server can then provide the VPN client the same enterprise address. By maintaining the association between the client and the enterprise address, the enterprise address can be provided to the same client at 815 even though the client is registering with a different subnetwork address. By maintaining the enterprise address, sessions are maintained at 819. [9:52-67-10:1-21]

Figure 8



With regard to claim 30, which teaches [30.3] "***a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second***

device", Leung does not expressly disclose such a DNS server, but the combination of Forslöw and Mehta does.

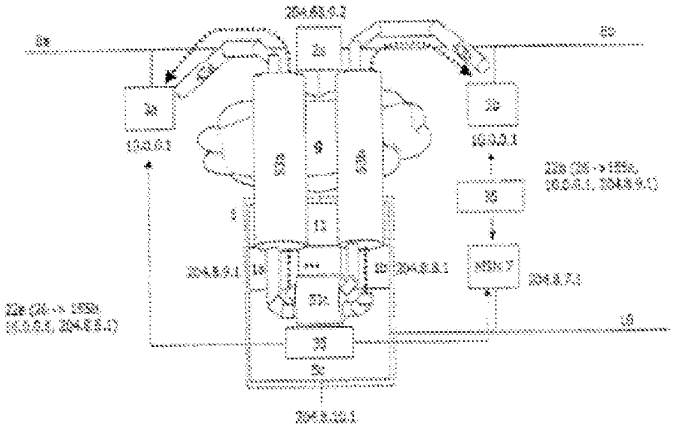
Forslöw

Forslöw discloses a virtual network (e.g., a mobile virtual network) that is defined by a domain name having an associated public network address (e.g., a user fully qualified domain name) [see Abstract], similar to that of Leung, and further teaches a DNS server for the virtual network (e.g., mobile service manager 7), the DNS server configured to receive a DNS request from a first device in the virtual network (e.g., mobile service manager 7 receives HTTPS request 22a from mobile node 3a), and return a private network address associated with a second device in the virtual network (e.g., the mobile node 3b private IP address 156b (10.0.0.1)), and a virtual network address associated with the second device (e.g., the virtual home agent's 1b public IP address 157b (204.8.9.1)).

A POSITA would have understood that Forslöw's mobile service manager 7 functions as a DNS server by receiving HTTPS requests from mobile nodes 3a and/or 3b and returning "user fully qualified domain name 155b/155a, the mobile node 3 private IP address (10.0.0.1) and the virtual home agent's 1a/1b public IP address (204.8.9.1 and 204.8.8.1 respectively)." Ex. 1006, 7:2-8. This functionality is similar to the VCN Manager disclosed as the DNS server in the '785 Patent, which receives a DNS request and returns a response including "the public IP address for private Route Director 2204, the private IP address for member M1 and the virtual IP address for member M1," and in some embodiments, a token key. Ex. 1001, 31:24-33.

- FIG. 2 shows the tunnel structure that is established in order to allow two mobile nodes 3a and 3b to be part of the same extranet workgroup in a secure manner. Note that both mobile node 3a and 3b are given the IP address 10.0.0.1 as their mobile virtual private networks have overlapping address realms. The foreign agent 2a is given a public IP address 204.68.9.2 as is the two virtual home agents 1a and 1b. Virtual home agent 1a has IP address 204.8.9.1 and virtual home agent 1b has IP address 204.8.8.1. Equally important is that the mobile service manager 7 is given a public IP address 204.8.7.1 that is unique across both mobile virtual private network realms. [9:62-10:6]

Fig. 2



- The home agent 1 also contains a backbone virtual router 5c that act as the common gateway towards the Internet 6 for all virtual home agents 1a and 1b. The backbone virtual home agent Sc also hosts a management network 10 to which a mobile service manager 7 for the mobile workgroup system is attached.

The mobile service manager 7 contains among other things a portal for workgroup membership list retrieval. The workgroup membership list is used in this invention to handle communication between workgroup members belonging to different address realms (mobile virtual private networks). However, it has also a more general appeal as a member list for creating any type of conference calls within the workgroup (e.g. by using Microsoft Netmeeting) [9:30-43]

- The mobile nodes 3a and 3b that are belonging to an extranet workgroup retrieve a list of workgroup members 26 by doing HTTPS requests 22a and 22 b to the mobile service manager 7 and its portal. For each workgroup participant a_ triplet including the user fully qualified domain name 155 b/155 a, the mobile node 3 private IP address 156 a/b (10.0.0.1) and the virtual home agent's 1a/1b public IP address 157 a/b (204.8.9.1 and 204.8.8.1 respectively). The triplets are retrieved at sign-on to the extranet workgroup and can be updated regularly through a push or pull procedure from the mobile service manager 7 portal. A network address port translator 35 in the backbone virtual router 5c allows for the traversal of the HTTPS requests 22a and 22b from the mobile nodes 3a and 3b to the mobile service manager 7. [10:7-20]

- FIG. 4a illustrates the registration procedure message flow when creating an extranet workgroup in a network-based mobile workgroup system, i.e. a workgroup with participants from more than one mobile virtual private network. The virtual home agents la and 1b are using the lightweight directory access protocol (LDAP) 25 to retrieve the extranet workgroup configurations. The virtual

home agent la sends an LDAP request 25a to the mobile service manager 7. The mobile service manager 7 replies with an LDAP answer 25b including any static routes 63 and filter states 64 to be applied to the workgroup traffic. [10:54-64]

- The mobile nodes 3a and 3b within the extranet workgroup asks for the workgroup member list 26 as part of a HTTPS request 22 a/22 b. The mobile service manager 7 responds with giving the triplets (the user fully qualified domain name 155 and private IP address 156 of the mobile node 3 as well as its virtual home agent 1 public IP address 157) for each workgroup member. This means that mobile node 3a receives the triplets for mobile node 3b and vice versa. [11:9-17]

- As in the normal mobile IP registration procedure, the mobile node 3a sends a registration request 46a with only its MAC address 5la as source and its virtual home agent la as destination to the foreign agent 2a. The foreign agent 2a forwards the registration request 46b further to the virtual home agent la. The registration reply 47a is sent from the virtual home agent la to the foreign agent 2a and forwarded to the mobile node 3a in the form of registration reply 47b. The next sequence shows the corresponding procedure for mobile node 3b. Note that both mobile nodes are capable of using the same foreign agent 2a. [11:18-28]

- The center module of a virtual home agent 1a/b is the virtual router 5 a/b. The virtual router is making nexthop decisions for datagrams passing through the virtual home agent 1 a/b. It is realm-specific to the mobile virtual private network that the virtual home agent 1a/b belongs to, and in such away can only route

packets that either has public destination IP addresses or private IP addresses that belong to the address realm of its mobile virtual private network. [12:14-2]

- The mobile service manager (MSM) 7 for a company will typically be placed at the WAN distribution layer 36 in order to be accessible from the inside as well as from the outside. From a network perspective it will function as a centralized data store from which the mobility routers 31 can fetch user and workgroup profiles. From a management viewpoint, it will be the portal to which the IT-administrator and workgroup members login for managing profiles and exchanging service information. [15:57-65]

Mehta

While Forslöw discloses a route director (e.g., router dispatcher 11), it does not explicitly disclose that the DNS server for the virtual network returns a network address associated with the network route director. Mehta discloses, or at least renders obvious a DNS server for the virtual network (e.g., a DNS'/API server of the Address Management Proxy System), the DNS server configured to receive a DNS request from a first device in the virtual network (e.g., DNS'/API server receives a request from a device on a public network), and return a network address associated with a network route director (e.g., the DNS'/API server returns the determined public network address of the associated Address Proxy /Router machine).

The address of the proxy/router machine returned in Mehta is a public address. Similarly, in the '785 Patent the network address associated with the network route director is a public address. See, e.g., Ex. 1001, 14:23-46.

Furthermore, to the extent it is determined that Forslöw's mobile service manager is not a DNS server, it would have been obvious to a POSITA to implement it as a DNS server, as disclosed in Mehta, with the functionality to return the same addresses in the triplet disclosed in Forslöw, as well as the public IP address for the route director, as disclosed in Mehta.

- In one embodiment, the AMPS comprises one or more modified DNS/API servers, one or more Address Proxy/Routers, an Address Management Data Server, one or more Address Management Data Repositories, and optionally a load balancer. The AMPS DNS'/API server receives a request from a device on a public network for a particular wireless device. And returns an appropriate temporary public address, which is internally mapped to the private address of the wireless device. The public address is then usable by the device on the external public network to send data to the wireless device. The temporary public address is, for example, an address associated with one of the Address Proxy/Routers, which are connected to the external public network and have access to the private addresses on the private wireless network. In some cases, the device on the public network that desires to send data to the wireless device uses a connection-based protocol, such as TCP/IP to send data. In other cases

the device uses a connection-less protocol, such as UDP (UDP/IP) to send the data. [0012]

- In operation, when a wired device such as wired device 201, desires to send data to wireless device 240, the wired device needs first to determine a routable address location of the wireless device 240 on the public network 210. However, as can be observed from FIG. 2, the wireless device 240 is not directly connected to the public network 210. Thus, the wired device must use the Address Management Proxy System 220 to determine a routable (public) address to which to send the data destined for the wireless device 240. To accomplish this task, the wired device 201 performs a query (for example, a modified DNS query) to locate a routable public address that corresponds to wireless device 240. The Address Management Proxy System 220 receives the query and determines and assigns a public (routable) address from a pool of addresses, which address can be used as a destination address for data packets targeted to wireless device 240. One should note that, although shown here as a DNS query, the Address Management Proxy System, as will be described further, modifies the DNS query implementation to handle wireless device technology, and/or provides an alternative API for determining a suitable routable address. Once the Address Management Proxy System 220 has returned a routable address to wired device 201, the wired device 201 can send data to that address. [0031]

- FIG. 3 is an example block diagram of components of an example Address Management Proxy System. In one embodiment, the Address Management Proxy System (AMPS) comprises one or more modified DNS'/API servers 302, one or more Address Proxy/Routers 305, an Address Management Data Server 303 which manages a database or other repositories such as Address Management Data Repository 304. and optionally a load balancer 301. The DNS'/API servers 302 are either individually connected to a public network 310 or are connected to the load balancer 301 which is in turn connected to public network 310. Similarly, each Address Proxy/Router 305 is also connected to the public network 310, via the routable (public) address to which data from the external network 310 is sent that is destined for the wireless devices. The DNS'/API servers 302 are either modified implementations of a DNS server to add functionality necessary to communicate with wireless devices, or are servers that implement one or more specialized APIs, as will be described further below. The DNS'/API servers 302 use the Address Management Data Server 303 to assist in mapping a unique identifier (e.g., string name) for a wireless device to a public address on public network 310. The pool of public addresses is also maintained by the Address Management Data Serve 303 and Data Repository 304. The Address Management Data server 303 and Address Management Data Repository 304 may be implemented using existing database technology, for example, ODBC technology or, may be implemented as a structure such as a simple text file. One skilled in the art will recognize that any embodiment for storing a set of tables, data, lists, or map pings can be used. Each Address

Proxy/Router 305 also uses the Address Management Data Server 303 or equivalent to create and update a series of routing tables that are used to assign public addresses to wireless devices as needed and to update the various mappings between public addresses and the non-routable (private) addresses of the wireless devices. The tables and mappings that are maintained on behalf of the DNS'/API servers 302 and the Address Proxy/Routers 305 by the Address Management Data Server 303 are described below with reference to FIG. 6.

[0032]

- FIG. 7 is an example flow diagram of an example routine provided by a DNS'/API server of the Address Management Proxy System to return a public address that corresponds to a designated unique identifier. In essence, this routine implements a DNS query or DNS- like query capability for the AMPS using a _ modified GetHostByName interface or a specialized API, for example GetProxyIP, as described with reference to FIG. 5. In summary, the routine dynamically allocates an appropriate Address Proxy/Router machine to associate with the wireless device and returns the public address of that machine (along with a TTL parameter and potentially other parameters). Specifically, in step 701, the routine determines the private (non-routable) address of the wireless device designated by a string parameter passed as input to the routine. For example, the string parameter may use fields such as "uniqueID.hostname.domain.tld," which specifies a typical hierarchy of person/service on a machine named "hostname" on a domain such as a company's network on a top level domain such as ".org", ".com", ".edu", etc. One skilled in the art will recognize that many

other string parameter designations could be used. One mechanism for implementing this routine is to request information from the Address Management Data Repository. In one embodiment, the data repository stores a table that maps unique IDs to private network addresses (see Table 610 in FIG. 6). Preferably, any mechanism that is used by the AMPS stores this data in a secure manner in order to keep the wireless network addresses private. In step 702, the routine retrieves the public network address that corresponds to the private wireless network address of the designated device if one has already been assigned by the AMPS to that device and is still valid. In one embodiment, the data repository stores this mapping information between private wireless network address and public network address (see for example table 630 in FIG. 6). If a public network address has not already been assigned or is not valid, then the routine causes a new public network address to be allocated and that new public address is associated with the private wireless network address. Appropriate tables in the data repository are then updated. In step 703, the routine determines the Address Proxy/Router machine that is associated with the assigned public network address (for example using table 620 in FIG. 6). In step 704, the routine sends a request to the determined proxy/router machine to update its routing tables to map the determined public network address to the private wireless network address. In step 705, the routine updates information in the data repository to include any other connection related information (e.g., field 634 in Table 630 in FIG. 6) and indicates a Time to Live (TTL) parameter for the public-private address association (e.g., field 633 in Table 630 in FIG. 6). Once

all of the tables have been updated in both the proxy/router and in the data repository, the DNS'/API server returns the determined public network address of the associated Address Proxy /Router machine. As described earlier, the public address may be a (hostname, port) pair when a port-based implementation is used. [0057]

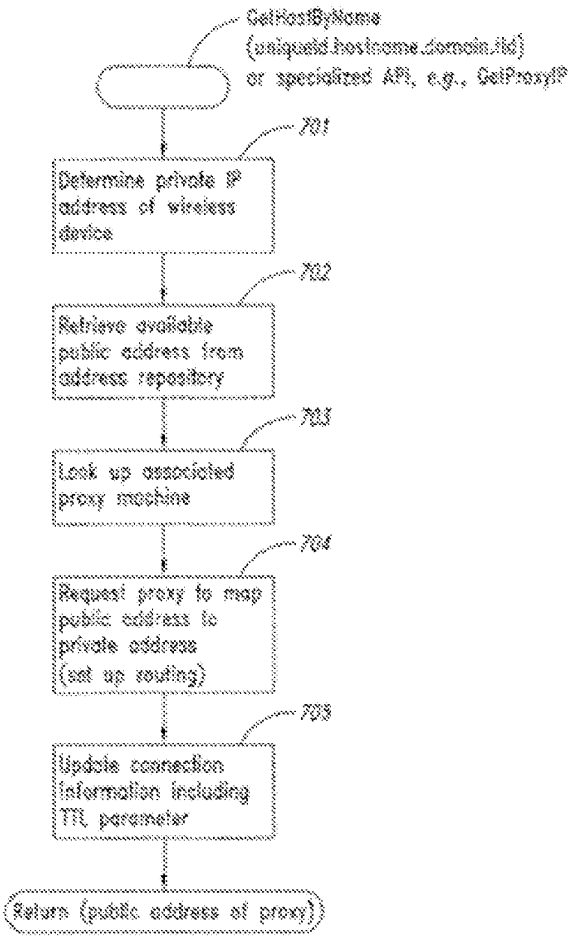


Fig. 7

- FIG. 8 is an example flow diagram of an example routine within an Address Proxy/Router of an example Address Management Proxy System that receives data. This routine is implemented by an Address Proxy/Router to receive data from wired devices using the relevant protocol (e.g., TCP/IP, UDP/IP, etc.). (Data is sent to a particular Address Proxy/Router because the public (routable) address of that Address Proxy /Router was returned to the requesting/ source device in response to a query of the DNS'/API server of the AMPS.) The proxy/router is responsible for any conversions of the data necessary to send data from the wired network to the wireless network (if, for example, the carrier infrastructure desires such conversion to be performed at this level). The proxy /router is also responsible for forwarding the data via the wireless network to the private wireless address of the wireless device that corresponds to the public address used to invoke the proxy/router. [0058]

Motivations to Combine Leung, Forslöw, and Mehta

It would have been obvious to a POSITA to incorporate Forslöw's and Mehta' s teachings related to a communication across virtual networks into Leung' s virtual private network system. Leung discloses a VPN system in which client devices gain access to the VPN in order to send data to devices within the VPN. See, e.g., Ex. 1005, 5:8-18. Forslöw discloses a similar VPN, but specifically details the way in which the DNS server (which it calls a mobile service manager) facilitates communication over the VPN system. See, e.g., Ex. 1006, 9:62-10:20. A POSITA would have been motivated to

make such a combination because implementation of Forslöw's VPN tunnelling system would have allowed data messaging to be sent in a more efficient and secure manner.

Additionally, Forslöw's VPN system provides for a virtual route director to assist in data mapping. See, e.g., Ex. 1006, 9:19-29. Mehta discloses a similar virtual networking system that operates with a DNS server and a route director, but it goes into more details about the operation of the route director, and thus provides for such DNS servers to provide private to network address associated with a network address proxy machine. See, e.g., Ex. 1007, [0012], [0031]-[0032]. A POSITA would have been motivated to make this combination because implantation of Mehta' s utilization of the DNS server would have aided in the security of the VPN system created by the combination of Leung and Forslöw.

Furthermore, a POSITA would have been motivated to combine Leung, Forslöw, and Mehta because the combination merely uses a known technique to improve similar devices in the same way. See KSR Intern. Co. v. Teleflex Inc., 550 U.S. 398, 401 (2007). For instance, the combination would have merely required the use of a known technique, specifically the utilization of routing via addresses provided by a DNS server to similar VPN systems in the same way.

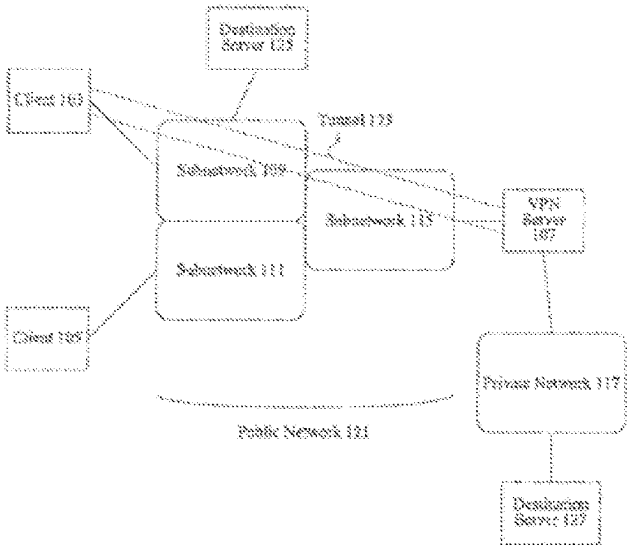
A POSITA would have had a reasonable expectation of success in modifying Leung's VPN system, which allows for registration and data transmission by client devices, to perform this data transmission via use of a DNS server and route director, as taught by Forslöw and Mehta, because doing so would merely have implemented a well-known technique in the VPN system of Leung, as shown above.

With regard to claim 34, which teaches [34.0] "***wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network***", See mapping of elements [30.2] and [30.3], above, for how Leung discloses a register module that is configured to receive a registration request from an agent associated with a device. Leung discloses the register module (e.g., software on CPU 1062) is further configured to receive the registration request (e.g., access request) from the agent that is installed on the device (e.g., software on the VPN client) for data communication via the virtual network (e.g., sending a data packet via the VPN).

- However, client 103 cannot access a private network destination server 127 until it is granted access by VPN server 107. To acquire access to destination server 127 in a private network 117, a client typically sends a request to set up a VPN tunnel or an access request to the VPN server 107. In the access request, the client 103 provides information such as its subnetwork address, its user name, and its password. [5:11-18]

- In one example, a client 103 may be a laptop attempting to access a company private network 117 through public network 121 and VPN server 107. [4:67-5:33]

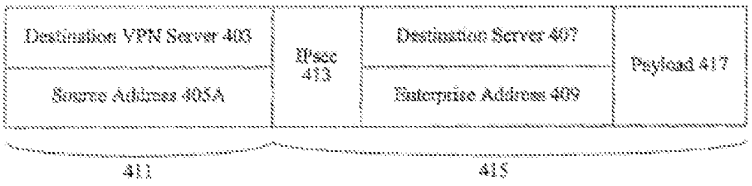
Figure 1



- In this example, the encapsulated portion 415, however, is typically encrypted using IPsec 413. Encapsulated portion 415 provides the VPN tunnel with security. More particularly, security is provided through enabling authentication of the sender (e.g., via information in the encapsulated portion 415) and encryption of data as well. For instance, the encapsulated portion 415 preferably contains the enterprise address 409 allocated by the VPN server to the VPN client during the creation of the VPN tunnel, which may be used to authenticate the sender. The encapsulated portion 415 also contains the destination address of the server 407 that the client wishes to access. In one example, the destination server 407 may be a Web server containing a page that the client wishes to view. The encapsulated portion 415 may also contain a payload 417. [6:53-67]

- FIG. 4A is a diagrammatic representation of a message that can be sent from a client to a destination when a VPN tunnel is used. [6:41-43]

Figure 4A



A POSITA would have understood that Leung's VPN clients would send registration requests via an associated agent. The '785 Patent describes "communication agent[s] installed on a device" that can include "software or hardware" and "may comprise a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address." Ex. 1001 at 7:1-8. Similarly, a POSITA would have understood Leung's VPN clients to include software to allow for traffic to be routed to members of the virtual community. This software would have been required for such a client device to send an access request to the VPN server. Thus, a POSITA would have understood that Leung discloses an agent associated with a device.

Summary

Claims 30 and 34 are REJECTED.

Claim 1-29, 31-33, and 35-90 is NOT SUBJECT TO REEXAMINATION.

Conclusion

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

In order to ensure full consideration of any amendments, affidavits or declarations, or other documents as evidence of patentability, such documents must be submitted in response to this Office action. Submissions after the next Office action, which is intended to be a final action, will be governed by the requirements of 37 CFR 1.116, after final rejection and 37 CFR 41.33 after appeal, which will be strictly enforced.

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent throughout the course of this reexamination proceeding. The requester is also reminded of the ability to similarly appraise the Office

of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP § § 2207, 2282, and 2286.

All correspondence relating to this ex parte reexamination proceeding should be directed:

Electronically: Registered users may submit via Patent Center at https://patentcenter.uspto.gov/.

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

By FAX to: (571) 273-9900
Central Reexamination Unit

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

For electronic transmissions, 37 CFR 1.8(a)(1)(i)(C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the USPTO patent electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication should be directed to Central Reexamination Unit at telephone number (571) 272-7705.

/DENNIS G BONSHOCK/
Primary Examiner, Art Unit 3992

Conferees:
/ROBERT L NASSER/
Primary Examiner, Art Unit 3992

/ALEXANDER J KOSOWSKI/
Supervisory Patent Examiner, Art Unit 3992

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Previous Prosecution History	06/11/2024	DGB
Litigation History	06/11/2024	DGB
Patent Data Portal	06/11/2024	DGB
P-TACTS	06/11/2024	DGB

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

AA/SWA Ex. 1015, p.543 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/019,519	**11/27/2024 10:24:19 AM Z ET**	**IVIPR-RE90019519**

Title of Invention

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	7949785
CONFIRMATION #	2698	FILED BY	Heather King
PATENT CENTER #	68145120	FILING DATE	05/22/2024
CUSTOMER #	3624	FIRST NAMED INVENTOR	- 7949785
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brandon Theiss

Documents

TOTAL DOCUMENTS: 2

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
IVIPR_RE90019519_RequestforEOT_PC.pdf		4	-	178 KB
IVIPR_RE90019519_RequestforEOT_PC-RXRQ/T.pdf	(1-3)	3	Reexam Request for Extension of Time	174 KB
IVIPR_RE90019519_RequestforEOT_PC-RXC/SR.pdf	(4-4)	1	Reexam Certificate of Service	105 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
IVIPR_RE90019519_RequestforEOT_PC.pdf	F4AAEA00ACBF412F22C111450515B47FEE657C5574BAAD3CA03E6D397B83FA2D1C2C5014FB852FBF5C5A249A213AFCC78D187EFEBF8988E75D32FBED4B856259

IVIPR_RE90019519_RequestforEOT_PC-RXRQ/T.pdf	1192DF0E293306562502ECDD07E359A848E16E03C91765822298255D586C221EA99361BA2A676E58EDA0E5315A375AB6F380DEAD1CDFAE60F9D3046D650A0E9A
IVIPR_RE90019519_RequestforEOT_PC-RXC/SR.pdf	7E74FADAC28FEF5AA0E6BA00611A7431752FFBD21387A09D8F3C79878A7AECDF950108D4540DDC2FA1EE95965F2CB088BEE67B094ADB66104ADE1B6FC848015E

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/019,519	**11/27/2024 10:24:19 AM Z ET**	**IVIPR-RE90019519**

Title of Invention

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	7949785
CONFIRMATION #	2698	FILED BY	Heather King
PATENT CENTER #	68145120	AUTHORIZED BY	Brandon Theiss
CUSTOMER #	3624	FILING DATE	05/22/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	- 7949785

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 4849	**E2024AQA24495812**	**Heather King**

PRE-AUTHORIZED ACCOUNT	PRE-AUTHORIZED CATEGORY
220493	**37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees)**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1251	EXTENSION FOR RESPONSE WITHIN FIRST MONTH	220.00	1	220.00
			TOTAL AMOUNT:	**$220.00**

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 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.

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R 1.550(f), the undersigned hereby certifies that a copy of Patent Owner's **Request for One Month Extension of Time Pursuant to 37 C.F.R. § 1.550(c)** is being served on November 27, 2024 to Third Party Requester via first class mail to:

Unified Patents, LLC
4445 Willard Ave., Suite 600
Chevy Chase, MD 20815

Date: November 27, 2024

By: /Brandon R. Theiss/
Brandon R. Theiss
Registration No. 70,507

AA/SWA Ex. 1015, p.548 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the ***Ex Parte Reexamination*** of:	
	Alkhatib et al.
Reexam Control No.:	90/019,519
Filed:	May 22, 2024
Patent No.:	7,949,785
Issued:	May 24, 2011
Confirmation No.:	2698
For: Secure Virtual Community Network System	
Group:	3992
Examiner:	Dennis G. Bonshock

Date: November 27, 2024

REQUEST FOR ONE MONTH EXTENSION OF TIME PURSUANT TO 37 C.F.R. §1.550(c)

Mail Stop *Ex Parte* Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Patent Owner respectfully requests a one (1) month extension of time to respond to the October 8, 2024 Non-Final Office Action in the above-identified reexamination proceeding. The current deadline is December 8, 2024, and the requested extension would move this deadline to January 8, 2025. This is Patent Owner's first request for an extension in this proceeding.

As discussed below, sufficient cause exists for the granting of the present request.

The present reexamination is directed to U.S. Patent No. 7,949,785 (the '785 Patent) and was filed by Unified Patents, LLC (the "Requestor"). On October 8, 2024, the Examiner issued an Office Action rejecting claims 30 and 34 based on Leung, Forslow and Mehta. As noted in

AA/SWA Ex. 1015, p.549 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

the Office Action, the Requester supported its Request with an Expert Declaration from Michael Shamos, which the Examiner considered in connection with the issuance of the Office Action and cited as providing "further rationale for the combination" of references applied in the rejection. Office Action, at 7.

On November 20, 2024, two other parties (Liberty Mutual and Comerica) filed a Petition for Inter Partes Review (IPR) challenging various claims of the '785 Patent, including claims 30 and 34, which was assigned IPR2025-00290. The IPR Petition is over 70 pages long and relies on a different prior art combination than applied in the Office Action. Specifically, the IPR Petition asserts that the claims of the '785 Patent are invalid based on a combination of Mehta and RFC-1383. *See* IPR2025-00290, Paper #3, at 3. In addition, the IPR Petition relies on the Expert Declaration of Dr. Erez Zadok, who has rendered different opinions from those advanced by Dr. Shamos in this reexamination.

Patent Owner previously enlisted a technical expert for assistance in this reexamination, and has been working with that expert in connection with the preparation of the response to the Office Action. However, due to the fact that the IPR was filed only a few days ago, and given the upcoming Thanksgiving Holiday which will occur shortly, Patent Owner and its expert are unable to both (i) fully analyze the substance of the IPR Petition and the Expert Declaration of Dr. Erez Zadok, and (ii) complete a response to the Office Action in these proceedings, between now and the current deadline (December 8, 2024) for responding to the Office Action.

These reexamination proceedings will be moving forward in parallel with the IPR, and positions taken by Patent Owner with respect to the '785 Patent in one proceeding may well be applicable to the other proceeding as well. Therefore, Patent Owner and its expert deserve a full opportunity to develop a comprehensive position why the claims of the '785 Patent are

AA/SWA Ex. 1015, p.550 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

distinguishable over all of the references cited in both proceedings before responding to the Office Action. The one-month extension now requested will provide Patent Owner and its expert the time necessary to perform this work.

Conclusion

In light of the above, Patent Owner respectfully submits that sufficient cause exists to grant it a one-month extension of time, extending the due date for filing Patent Owner's Response to the Office Action from December 8, 2024 to January 8, 2025.

The Petition fee in the amount of $220.00 (regular undiscounted) pursuant to 37 C.F.R. § 1.17(g) is enclosed. The Office is authorized to charge any underpayment of fees or additional fees for this Request to Deposit Account No. 22-0493.

Respectfully submitted,

By:/Brandon R. Theiss/
Brandon R. Theiss
Registration No. 70,507

Volpe Koenig
30 South 17th Street
Philadelphia, PA 19103-4009
(215) 568-6400

BRT/hlk

AA/SWA Ex. 1015, p.551 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

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.
90/019,519	05/22/2024	7949785	IVIPR-RE90019519	2698

3624 7590 11/29/2024

VOLPE KOENIG
30 SOUTH 17TH STREET, 18TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
11/29/2024	PAPER

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

11/29/2024

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS

UNIFIED PATENTS, LLC
4445 WILLARD AVE.
SUITE 600
CHEVY CHASE, MD 20815

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. : 90019519
PATENT NO. : 7949785
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Decision on Petition for Extension of Time in Reexamination	**Application No.:** 90/019,519	**Applicant(s):** 7,949,785	
	Examiner BONSHOCK, DENNIS	**Art Unit** 3992	

1. THIS IS A DECISION ON THE PETITION FILED November 27, 2024.

2. THIS DECISION IS ISSUED PURSUANT TO:
   - A. ☒ 37 CFR 1.550(c) – The time for taking any action by a patent owner in a third party requested *ex parte* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   - B. ☐ 37 CFR 1.550(c) – The time for taking action by a patent owner in a patent owner requested *ex parte* reexamination proceeding will only be extended for more than two months for sufficient cause and for a reasonable time specified.
   - C. ☐ 37 CFR 1.956 – The time for taking any action by a patent owner in an *inter partes* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.

   The petition is before the Central Reexamination Unit for consideration.

3. FORMAL MATTERS: Patent Owner requests that the time period for filing a response to the non-final Office action mailed on October 8, 2024, which set a two (2) month shortened statutory period for response, be extended by one (1) additional month.
   - A. Petition fee per 37 CFR § 1.17(g)):
     - i. ☐ Petition includes authorization to debit a deposit account.
     - ii. ☒ Petition includes authorization to charge a credit card account.
     - iii. ☐ Other: _____.
   - B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester).
   - C. ☒ Petition was timely filed.
   - D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)
   - A. ☒ Granted for: one additional (1) month or ☐ Granted-in-part for: __. (See 37 CFR 1.550(c) and 37 CFR 1.956).
     - i. ☐ Other/comment: _____.
   - B. ☐ Dismissed because:
     - i. ☐ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 3 above).
     - ii. ☐ Petitioner failed to provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.
     - iii. ☐ Petitioner failed to explain why, in spite of the action taken thus far, the requested additional time is needed.
     - iv. ☐ The statements provided fail to establish sufficient cause to warrant extension of the time for taking action (See attached).
     - v. ☐ The petition is moot.
     - vi. ☐ Other/comment: _____.

5. CONCLUSION:

Direct telephone inquiries to either QAS Stephen J. Stein at 571-272-1544 or SPRS Andrew J. Fischer at 571-272-6779.	/Andrew J. Fischer/, Supervisory Patent Reexamination Specialist, Central Reexamination Unit

AA/SWA Ex. 1015, p.554 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the ***Ex Parte* Reexamination** of Intellectual Ventures I LLC **Reexam Control No.:** 90/019,519 **Confirmation No.: 2698** **Filed:** May 22, 2024 **Patent Number:** 7,949,785 **Issued:** May 24, 2011 **For**: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM **Group:** 3992 **Examiner**: DENNIS G BONSHOCK	Our File: IVIPR-RE90019519 Date: January 8, 2025

RESPONSE TO OFFICE ACTION IN EX PARTE REEXAMINATION

Mail Stop *Ex Parte* Reexam
Central Reexamination Unit - EFS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This Response is being timely filed in response to the October 08, 2024 Non-Final Office Action, and the Decision on the Request for Extension of Time granted on November 29, 2024.

AA/SWA Ex. 1015, p.555 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

TABLE OF CONTENTS

PATENT OWNER'S EXHIBIT LIST iii

I. Status of Claims 1

II. Example of the Invention 1

III. Response to Claim Rejections 3

A. Mehta, Forslow, And Leung, Alone Or In Combination, Fail To Teach Or Suggest A "Domain Name" As Recited In The Challenged Claims. 3

B. Mehta, Forslow And Leung, Alone Or In Combination, Fail To Suggest A DNS Server As Recited In The Challenged Claims. 11

C. The Office Action Improperly Conflates "Registration" and "Join" Processes, Failing to Establish That the Cited References Teach the Claimed Registration. 21

IV. Conclusion 25

AA/SWA Ex. 1015, p.556 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

PATENT OWNER'S EXHIBIT LIST

Ex. 2001	Declaration of Dr. Guevara Noubir
Ex. 2002	Microsoft® Computer Dictionary, Fifth Edition 5th ed.
Ex. 2003	Searing, Matthew Edward. "What's in a Domain Name - A Critical Analysis of the National and International Impact on Domain Name Cybersquatting." Washburn Law Journal, vol. 40, no. 1, Fall 2000, pp. 110-142. HeinOnline
Ex. 2004	DHCP for Windows 2000: Managing the Dynamic Host Configuration Protocol 1st Edition by Neall Alcott
Ex. 2005	IETF RFC 2131- Dynamic Host Configuration Protocol
Ex. 2006	Designing ISP Architectures by John V. Nguyen
Ex. 2007	IETF RFC 1035 – Domain Names – Implementation and Specification
Ex. 2008	IETF RFC 2818 - HTTP Over TLS

AA/SWA Ex. 1015, p.557 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

UNITED STATES PATENT AND TRADEMARK OFFICE

In the *Ex Parte* Reexamination of

U.S. Patent No. 7,949,785

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

INTELLECTUAL VENTURES I LLC,
Patent Owner.

Reexam Control No. 90/019,519

DECLARATION OF DR. GUEVARA NOUBIR

AA/SWA Ex. 1015, p.558 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

TABLE OF CONTENTS

I. QUALIFICATIONS 1

II. SCOPE OF WORK 3

III. OPINION 4

A. LEGAL STANDARDS 4
B. LEVEL OF SKILL OF A PERSON HAVING ORDINARY SKILL IN THE ART 5
C. SUMMARY OF MY OPINIONS 6
D. BRIEF SUMMARY OF '785 7
E. LEUNG '143, FORSLÖW '518, AND MEHTA '671 DO NOT TEACH CLAIM 30 OF THE '785 PATENT 8
F. THE COMBINATION OF LEUNG '143, FORSLÖW '518, AND MEHTA '671 DOES NOT TEACH CLAIM 34 OF THE '785 PATENT 24

IV. CONCLUSION 27

I. QUALIFICATIONS

1. My name is Guevara Noubir. I am employed at Northeastern University as a Professor in the Khoury College of Computer Sciences.

2. I hold an M.S. in Computer Science (diplôme d'ingénieur) from the Ecole Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble (ENSIMAG) and Institut National Polytechnique de Grenoble (INPG), France, with a specialization in networks and real-time systems. I hold a Ph.D. in computer science from the Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland. One of my primary fields of study in graduate school was algebraic methods for fault tolerance in the context of communications network protocols.

3. For three years, after my PhD, I worked as a senior research scientist in the Real-time Software and Networking Group at the Centre Suisse d'Electronique et de Microtechnique (CSEM) in Switzerland. My responsibilities included coordinating several European projects in wireless communications and network security.

4. I have been a professor of computer science at Northeastern University since 2001, and a full Professor since 2011.

5. In my first full-time academic position (Assistant Professor) at Northeastern University, I taught in the areas of computer networks and wireless networks. I have taught courses on Internetworking and Wireless Networks since 2001. I introduced and began teaching courses in network security in 2003. In 2005, I began teaching a course in cryptography.

6. I have published and lectured extensively, primarily focusing in the areas of networks and wireless systems security, including new frontiers in networking, robustness

and privacy in wireless and mobile systems, secure sharing of location information in wireless networks, preventing hacking of wireless networks, directing wireless security research, game theory in the wireless adversarial context, challenges to wireless security, heterogeneous wireless networks, wireless infrastructure, scalability and security of wireless networks, securing wireless sensor networks, and security challenges of multihop ad hoc networks.

7. I was named an IEEE Senior member in 2001 and have received numerous awards and honors for my research, including the US National Science Foundation CAREER Award in 2005, Google Faculty Research Award on Privacy in 2016, Northeastern University Excellence in Research and Creative Activity Award in 2018, best paper awards at ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) in 2011 and 2018, and the IEEE Conference on Communications and Network Security best paper in 2016.

8. I led winning teams from Northeastern University in the DARPA Spectrum Collaboration Challenge (SC2) in 2017, 2018, and a finalist team in 2019.

9. I delivered keynote lectures at the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2019), and IEEE Conference on Communications and Network Security (CNS 2022).

10. I chaired the technical program committee of several academic conferences including the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2015), and IEEE Conference on Communications and Network Security (CNS 2015). I served on the editorial boards of ACM Transaction on Privacy and Security, IEEE

Transactions on Mobile Computing, Elsevier Journal on Computer Networks, and IEEE Transaction on Information Forensics and Security.

11. A copy of my CV is attached as Appendix A.

12. I have been retained by Volpe Koenig to provide various opinions regarding the '785 patent.

13. I do not have any other current or past affiliation as an expert witness or consultant with Volpe Koenig. I do not have any financial interest in the outcome of this proceeding.

14. I am being compensated at my normal consulting rate for my time. My compensation is not dependent on and in no way affects the substance of my statements in this Declaration.

II. SCOPE OF WORK

15. I reviewed the specification, claims, and file history of US patent 7,949,785 issued to Alkhatib et al. (hereinafter the '785 Patent). I understand that the '785 Patent was filed on March 31, 2003.

16. I have reviewed the ex parte reexamination communication document 90/019,519, the declaration by Dr. Michael Shamos, as well as US Patents No. 7,036,143 (Leung), No. 7,155,518 (Forslöw), and No. 2003/0028671 (Mehta).

17. I was asked to provide my opinion on claim 30 and claim 34. Specifically, if the combination of Leung '143, Forslöw '518, and Mehta '671 renders claims 30 and 34 of '785 obvious.

III. OPINION

A. Legal Standards

18. I am not an attorney. However, I have been informed by counsel of certain legal standards and have applied those standards, described below, in formulating my opinions.

19. I understand that the claims of a patent define the limits of a patentee's exclusive rights. I understand that to determine the scope of the claimed invention, courts may construe claim terms, the meaning of which the parties may dispute. I understand that claim terms should generally be given their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of filing of the patent application.

20. I understand that claims must be construed in light of and consistent with the intrinsic evidence. In this context, I understand that intrinsic evidence includes the claims themselves, the written disclosure in the specification, and the patent's prosecution history. I understand that the specification is always highly relevant to the claim construction analysis and often is the single best guide to the meaning of a disputed term. I understand that extrinsic evidence may also be considered when construing claims and may include, for example, technical dictionaries, technical publications and books, treatises, and expert testimony, though the intrinsic record will be more persuasive as to the meaning of a particular term.

21. I understand that one or more prior art references can render a patent claim obvious to a person of ordinary skill in the art if the differences between the subject matter set forth in the patent claim and the prior art are such that the subject matter of the claim

would have been obvious at the time the claimed invention was made. In analyzing obviousness, I understand that it is important to consider the scope of the claims, the level of skill of a person of ordinary skill in the relevant art, the scope and content of the prior art, the differences between the prior art and the claims, and "secondary considerations" of non-obviousness, which I also understand can include, for example, evidence of commercial success of the invention, evidence of a long-felt need that was solved by an invention, evidence that others copied an invention, or evidence that an invention achieved an unexpected result.

22. I understand that the claimed subject matter can be obvious when a person of ordinary skill in the art would have been motivated to combine pre-existing elements, and that combination yields no more than what a person of ordinary skill in the art would have expected. I also understand that, in assessing whether a claim is obvious, one must consider whether the claimed improvement is more than the predictable use of prior art elements according to their established functions. I understand that there need not be a precise teaching in the prior art directed to the specific subject matter of a claim because one can take account of the inferences and creative steps that a person of ordinary skill in the art would employ. However, I further understand that obviousness cannot be based on the hindsight combination of components selectively culled from the prior art.

B. Level of Skill of a Person Having Ordinary Skill in the Art

23. I have been advised that the '785 patent application was filed on March 31, 2003, and issued on May 24, 2011.

24. I have been advised that a "person of ordinary skill in the art" (POSITA) is a hypothetical person to whom one could assign a routine task with reasonable

confidence that the task would be successfully carried out. I have been advised that the relevant timeframe is prior to March 31, 2003. When I refer to "March 2003," I am referring specifically to prior to March 31, 2003.

25. In my opinion, a person of ordinary skill in the art in March 2003 would have a bachelor's degree in computer science or electrical engineering, and would have one or two years of experience in computer networking or equivalent educational and professional experience. I base this opinion on my experience in the networking industry in general, and with computer networking specifically, in March 2003. At that time, those thinking about or developing improved systems or ways for secure communications networks would have at least this level of experience and knowledge.

C. Summary of My Opinions

26. Claim 30 of '785 recites a virtual network manager that comprises of a network interface configured for data communication via a **virtual network** that is **defined by a domain name** having an associated public network address. In my opinion, the combination of Leung, Forslöw, and Mehta does not disclose a virtual network defined by a domain name, or the use of DNS protocols.

27. Claim 30 of the '785 Patent also recites "a DNS server for the virtual network" that returns "a **private network address associated with a second device in the virtual network, and a virtual network address associated with the second device**." Leung, Forslöw, and Mehta do not teach that any server provides a response with **both a Virtual and a Private IP address** as thought by '785.

28. Claim 34 of the '785 Patent teaches a register module. The '785 Patent defines two distinct processes, one for registration and another process for Join/Leave.

"The registration process is the first step that a user and machine go through with the VCN Manager before becoming a member of a virtual community." The registration or access requests in the Leung, Forslöw, and Mehta references do not teach the functionality or steps of registration and defined by the '785 Patent and recited in Claim 34, as discussed in more detail below.

D. Brief Summary of '785

29. The '785 Patent teaches how multiple devices can be operated and managed to form dynamic virtual communities and streamline communications even if some/all are not on the same physical network. It is noteworthy that a traditional VPN does not enable such communications as two devices might connect from arbitrary physical networks, changing their IP addresses; the IP addresses can change as they can change physical networks; such devices might pass through NAT boxes and, therefore have private IP addresses but are seen by other devices as using the global IP address of the NAT box. The patent introduces a comprehensive architecture, components, hardware and software to build a Virtual Community Network (VCN) with other components to support routing and learning Virtual IP addresses to reach other devices (using DNS names). It operates as an overlay but with various management mechanisms and optimizations. It supports a range of connectivity/networking scenarios including NAT traversal, devices with public and private IP addresses, and Route Directors (PRD/NRDs). It integrates with the DNS protocols for the devices to determine how to reach each other. It supports secure tunnels in particular encrypted ones (IPsec/IKE). It supports devices that are not aware of the VCN but are bridged through a Group Agent (GA). It supports defining virtual communities' membership including

registration, and dynamic join/leave, authentication, and group policies. It supports multiple virtual communities.

E. Leung '143, Forslöw '518, and Mehta '671 do not teach Claim 30 of The '785 Patent

30. Claim 30 of the '785 Patent recites a virtual network manager that comprises of a network interface configured for data communication via a **virtual network** that is **defined by a domain name** having an associated public network address. In my opinion, there are two key reasons why Leung does not teach all of the elements of Claim 30.

31. First, the '785 Patent teaches that the **virtual network is defined by a domain name**. Leung discloses that "client 103 may acquire a subnetwork address from the Internet service provider associated with subnetwork 109." There is no evidence that the virtual network in Leung is defined by a domain name. A subnetwork address is defined by 4 bytes, for example 192.1.14.8 within a subnetwork defined by address 192.1.14.0 and a mask 255.255.255.0. As disclosed by Leung "In one example, a client 103 may wish to transmit a message to destination address 203 corresponding to 192.1.14.8". A typical VPN in 2003 operated without involving any DNS server. The focus of Leung is on a VPN access such that the client accesses enterprise resources and obtains the same IP address on re-connections to maintain sessions. In my opinion, a POSITA in 2003 reading Leung would not have concluded that the virtual network in Leung used a domain name, because the mere assignment of an IP address by an ISP does not require that there be an association with a domain name..

32. A person of ordinary skill in the art (POSITA) would recognize that a domain name is a human-readable identifier that corresponds to a specific location on the Internet, such as a website or an online service. It acts as an alias for an IP address, the numerical identifier that computers use to locate and access network resources. Domain names simplify navigation by enabling users to enter a recognizable name, such as example.com, instead of a complex numerical IP address. They are organized hierarchically into components separated by dots, such as www.example.com, where "www" is an optional subdomain, "example" is the second-level domain, and "com" represents the top-level domain (TLD). The Domain Name System (DNS) resolves these domain names into their corresponding IP addresses, facilitating communication between computers and the appropriate servers or devices.

33. A POSITA would also understand that an IP address (Internet Protocol address) is a unique numerical identifier assigned to each device connected to a network that uses the Internet Protocol for communication. It serves two primary purposes: identifying the host or network interface and providing the location of the device within the network, enabling data to be sent and received accurately. IP addresses come in two formats: IPv4, which uses a 32-bit address scheme (e.g., 192.168.1.1), and IPv6, which uses a 128-bit address scheme (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334) to accommodate a vastly larger number of devices. They can be dynamically assigned by a network's Dynamic Host Configuration Protocol (DHCP) or statically configured for specific devices. IP addresses are critical for routing data packets between devices on local networks or across the Internet, ensuring seamless communication and connectivity in modern digital systems.

34. IP addresses are assigned through either dynamic allocation or static assignment, depending on the network configuration. Dynamic allocation, the most common approach, is managed by a Dynamic Host Configuration Protocol (DHCP) server. When a device connects to a network, it sends a request to the DHCP server, which automatically assigns an available IP address from a predefined pool. This automated process ensures that devices are assigned unique IP addresses without requiring manual configuration. Significantly, this address assignment process does not require that the assigned IP address be associated with a domain name. The assigned address is typically leased for a specific period, after which the lease may be renewed, potentially resulting in a new address. This method is widely adopted in home and enterprise networks for its efficiency and ease of use. Conversely, static assignment involves manually configuring a specific IP address on a device, ensuring a consistent address that is ideal for devices requiring fixed identification, such as servers, printers, or security cameras. In scenarios where no DHCP server is present, devices can use Automatic Private IP Addressing (APIPA) to assign themselves an address within a predefined range (e.g., 169.254.0.0), enabling local communication but not external network access. For internet-facing devices, Internet Service Providers (ISPs) assign public IP addresses, which can be either static or dynamic. Again, nothing about such assignments requires an association between the assigned public IP address and a domain name.

35. Accordingly, the assignment of IP addresses is completely unrelated to the existence of a domain name. Therefore, there is nothing about the assignment of an IP address by an ISP to a device that requires the addressee to have a domain name or

even be a member of a domain. In fact, all computers connected to the Internet must have an IP address; however, the vast majority of those computers do not have a domain name, nor are they members of a domain.

36. In addition, a Virtual Private Network (VPN) is a secure communication technique that establishes a connection between a user's device and a remote server over the Internet, effectively simulating the functionality of a direct physical connection. There is absolutely nothing about a VPN that requires the existence of a domain or the connecting device to have a domain name. All a VPN enables is remote computers to act as if they are physically connected via a wire when they are in fact connected via the Internet.

37. Furthermore, combining Leung with Forslöw does not teach that the virtual network is defined by a domain name as required by claim 30 of the '785 Patent. Forslöw is aware of the meaning of a domain name, as it refers to a User Fully Qualified Domain Name (UFQDN), but the reference did not define its "network-based mobile workgroup system" by a domain name. Nor is there any reference to a **domain name server** in Forslöw. "They retrieve a list of workgroup members 26 by doing HTTPS requests 22a and 22b to the mobile service manager 7 and its portal." However, the mobile service manager is not a DNS server. The DNS protocol is very clearly defined by the Internet Engineering Task Force (IETF) in document RFC 1034 (and its companion document RFC 1035). In my opinion, a POSITA combining Leung and Forslöw would not have viewed the mobile service manager as a DNS server, but rather as a web application server accessible through the HTTPS protocol. DNS protocol runs on top of UDP or TCP and is lightweight, while HTTPS runs the HTTP protocol over TLS. Finally, even the

combination with Mehta does not teach that the **virtual network is defined by a domain name**.

38. Second, claim 30 of the '785 Patent teaches "a DNS server for the virtual network, the DNS server configured to **receive a DNS request** from a first device in the virtual network, and return a network address associated with a network route director, a **private network address associated with a second device in the virtual network, and a virtual network address associated with the second device**".

39. Forslow's mobile service manager 7 does not function as a DNS server that "is configured to receive a **DNS request**". Forslow states that "the mobile nodes 3 a and 3 b … retrieve a list of workgroup members 26 by doing **HTTPS requests** 22 a and 22 b to the mobile service manager 7 and its portal." (Forslow, 10:7-10). However, HTTPS requests are fundamentally different from DNS requests. The fact that a server receives an HTTPS request and resolves an IP address does make the sever a "DNS server" or the request a "DNS request," as claimed. . A DNS request is responsible for **resolving a domain name**, such as www.example.com, into its corresponding IP address (e.g., 93.184.216.34) to enable devices to locate and communicate with the server hosting the desired resource. Significantly, **a DNS request includes the domain name to be resolved**, and the response from the DNS server includes a numeric IP address. By contrast, the HTTPS request relied on from Forslow **lacks any domain name**.

40. DNS requests and HTTPS requests serve distinct functions in a computer network. A DNS request resolves a domain name, such as www.example.com, into its corresponding IP address (e.g., 93.184.216.34), allowing devices to locate and communicate with the server hosting the desired resource. The Domain Name System

(DNS) primarily utilizes the User Datagram Protocol (UDP) on port 53, a lightweight and efficient protocol that enables quick transmission of DNS queries and responses without requiring a persistent connection. DNS requests are small, typically involving a query for specific record types (e.g., A, AAAA, CNAME, MX) and a server response containing the requested information. Latency is further reduced through caching mechanisms at various levels, such as local resolvers, ISP servers, and content delivery networks (CDNs).

41. By contrast, HTTPS requests facilitate secure communication between a client (e.g., a web browser) and a server, leveraging the HyperText Transfer Protocol over an encrypted SSL/TLS connection. HTTPS operates at the application layer and relies on TCP at the transport layer, typically over port 443, to ensure reliable data delivery. The SSL/TLS handshake at the start of an HTTPS session establishes a secure communication channel by negotiating encryption algorithms, exchanging certificates, and deriving session keys. This process guarantees confidentiality through encryption, integrity by detecting tampering, and authentication by verifying the server's identity. HTTPS requests involve significantly more complex data exchanges than DNS requests, including HTTP headers, cookies, query parameters, and encrypted payloads such as sensitive user data or web content. This added complexity introduces higher latency due to the overhead of the TCP three-way handshake and SSL/TLS setup.

42. Therefore, HTTPS requests and DNS requests are completely different things. For example, the different types of requests operate on different ports, require/ don't require a persistent connection, and perform completely different functions.

43. LDAP is a protocol designed for accessing and managing directory information services over a network. It allows applications to query, search, and modify

hierarchical directories that store data about users, groups, devices, or other organizational resources. LDAP operates over TCP/IP, typically using port 389 for standard communication and port 636 for secure communication via SSL/TLS. It supports functions such as authentication, searching, and modifying directory entries, making it commonly used for user authentication, centralized access control, and resource management in systems like Microsoft Active Directory and OpenLDAP.

44. LDAP and DNS serve fundamentally different purposes and operate with distinct functionalities. LDAP focuses on managing and accessing directory-based information, such as user accounts, groups, and permissions, to enable authentication and access control in enterprise environments. In contrast, DNS is designed primarily to map human-readable domain names to IP addresses for efficient network routing. While LDAP facilitates the querying and modification of hierarchical directory structures, DNS resolves domain names to their corresponding network addresses. LDAP relies on TCP for reliable communication, typically using ports 389 or 636, and incorporates features like secure authentication, role-based access, and Single Sign-On (SSO) integration, which are unrelated to DNS's core function of domain name resolution.

45. Therefore, Forslöw's mobile service manager 7 is not "a DNS server for the virtual network that is configured to receive a DNS request" and "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device."

46. Forslöw's Figure 8 (reproduced below) illustrates a routine implemented by an Address Proxy/Router within an Address Management Proxy System (AMPS). This

routine manages data received from wired devices and facilitates communication with wireless devices by determining the private wireless address corresponding to the invoked public address. It ensures compatibility with the wireless network's requirements by validating the address mapping using a Time-To-Live (TTL) parameter, performing necessary protocol or format conversions, and forwarding the data to the wireless device's private address.

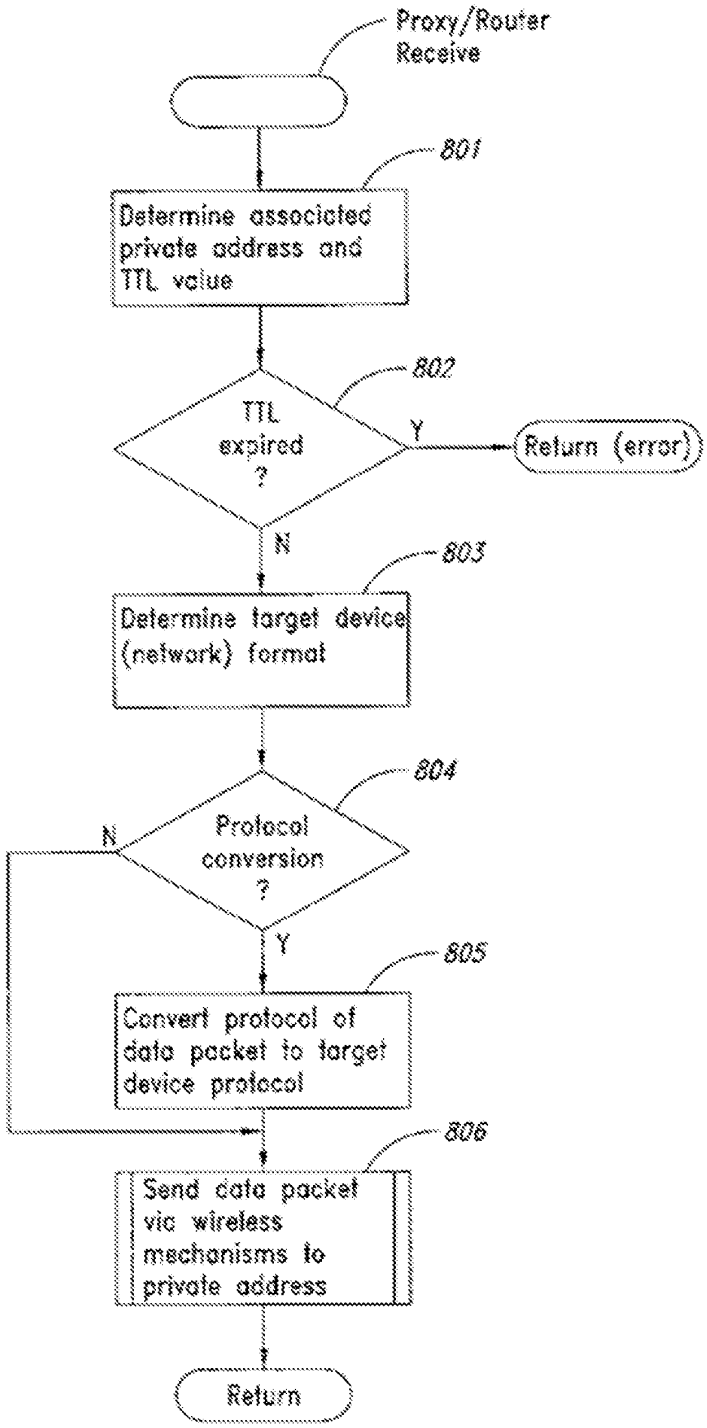


Fig. 8

AA/SWA Ex. 1015, p.575 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

47. However, in Mehta, the sender only learns the address of the Proxy/Router, with the Proxy/Router performing the address conversion. The sender does not have knowledge of both the route director and the virtual/private address of the destination. As a result, Mehta does not disclose or suggest the ability to "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device," as required by claim 30 of the '785 Patent. Instead, Mehta's architecture closely resembles the Dynamic DNS system depicted in Figure 3 of the '785 patent, which is explicitly labeled as prior art.

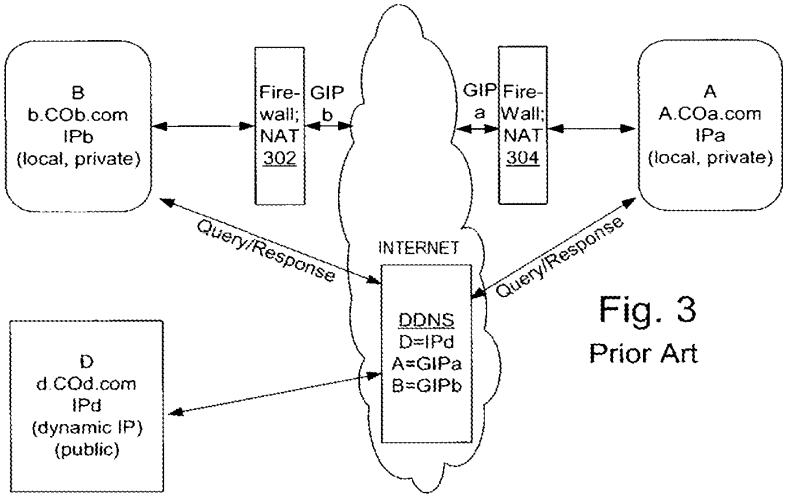


Fig. 3
Prior Art

48. Furthermore, providing all three addresses would contradict Mehta's primary goal of reducing security risks, as such disclosure would increase the vulnerability of the system.

49. At most, Mehta permits a client to obtain a temporary public IP address from a DNS server. However, the reference provides no guidance on addressing the problem solved by the current invention, specifically how to route through a route director to the

virtual address. Accordingly, Mehta does not disclose or suggest "a DNS server for the virtual network" configured to "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device."

50. In addition, Leung, Forslöw, and Mehta do not teach that any server provides a response with **both a Virtual and a Private IP address.** There are two reasons for providing both virtual and private IP addresses: (1) to allow direct communications between clients (residing in a private LAN) facilitated by their Member Agents ('785 Fig. 5B), and (2) to allow communications with a client whose Route Director is on a Private LAN (PRD) and therefore behind a NAT box.

51. **Direct communication between clients behind a NAT box.** This is illustrated in the '785 Patent at FIG. 5 and FIG. 5B, and also explained in the corresponding text. client M_C learns the **Private IP** address of client M_B (and vice versa) and can directly communicate with each other without going through external route directors. "FIG. 5B shows exemplary traffic between elements of the VCN. A first type of traffic is TCP traffic. TCP traffic is used between member agents to establish membership in the VCN (the registration process), and make the VCN manager aware that they are available to communicate with other members of the VCN (the join process). In FIG. 5B, this is represented by solid lines 513 b, 511 b, 523 b and 543 b. TCP is also used: by the PRD 530 to establish communications with the VCN (lines 527b, 527 d); and by the member agent of device M_B to communicate with the PRD 530 (line 533 b). TCP may also be used by devices M_C and M_D on private network 550 to communicate with each other."

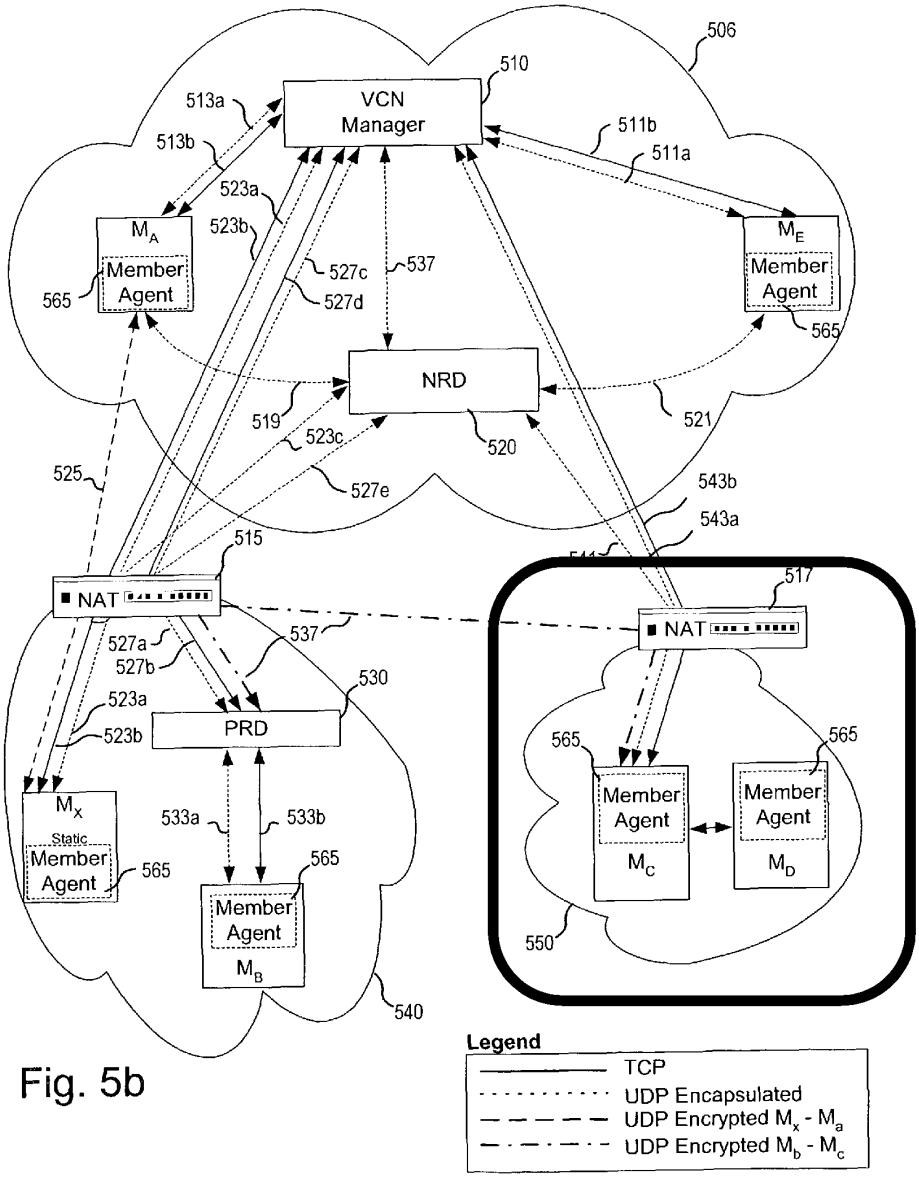
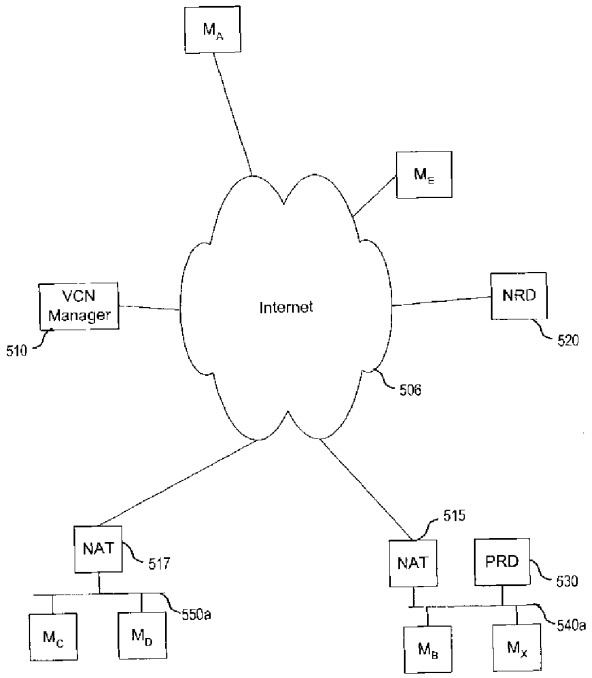


Fig. 5b

AA/SWA Ex. 1015, p.578 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Fig. 5a

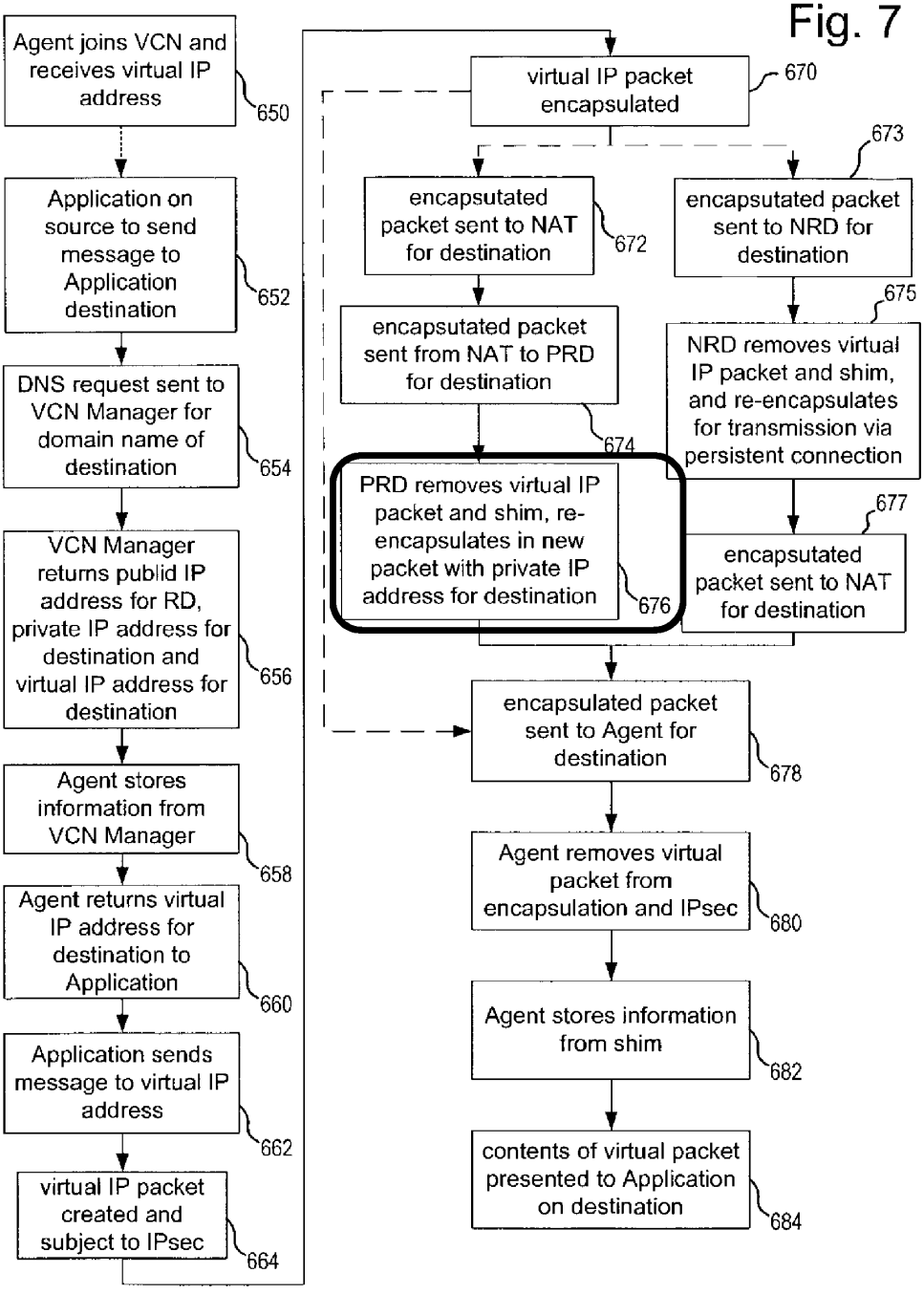


52. **Communication with a client whose Route Director is on a Private LAN (PRD) and therefore behind a NAT device.** FIG. 7 shows the use of a combination of Virtual Addresses and Private Addresses. The process is specifically shown in step 656, followed by steps 672, 674, and 676. The use is exemplified by a communication from M_A to M_B through a Private Route Director (PRD 530) located behind a NAT (515). M_A's agent using DNS obtains the Public Address of PRD (which is the IP Address of NAT 515), the Virtual Address of M_B and Private Address of M_B. There are three layers of encapsulation (built by M_A agent). In the first layer, the IP header has virtual source/destination addresses for M_A and M_B. A second layer consists of the shim containing the Public IP source/destination address of RD and Private Address of source/destination. Finally, an

IP header with public source of M_A and public IP of PRD which is the NAT device address. The '785 Patent states: "Consider an example when application on device M_A intends to initiate communication with an application on device M_B. Thus, M_A is the source device and M_B is the destination device. In step 654, the application on M_A will initiate a DNS request using the domain name for M_B. This DNS request is sent to VCN Manager 510. In step 656, VCN Manager 510 returns the public address of the Route Director for the destination, the **private address for the destination** device **and a virtual IP address for the destination** device. In the example described above, step 656 includes returning the public IP address for private Route Director 530, the private address for M_B and a virtual IP address for M_B. If the destination machine has a public IP address (and, thus, does not use a routing director) then step 656 will only include returning the public IP address for the destination. If the destination machine is in a private network that uses a Network Route Director (e.g., NRD 520), then step 656 will return the public IP address for the Network Route Director." … "If the destination is in a private network that has a PRD, then in step 672 the encapsulated packet is sent to the NAT device for the destination. For example, the encapsulated packet is sent from M_A to NAT 515. In step 674, the encapsulated packet is sent from the NAT device for the LAN that includes the destination to the Route Director for the destination. For example, the encapsulated packet is sent from NAT 515 to private Route Director 530. **In step 676, the Route Director which received the encapsulated packet will remove the virtual IP packet and the shim from the encapsulation. The Route Director will read the shim to learn the local IP address to send the packet to. The shim and virtual IP address will then be re-encapsulated into a new packet with the original virtual packet. The new outer**

packet includes a destination IP address equal to the private IP address of the destination device. The encapsulated packet received in step 674 will include a source IP address equal to the public IP address for MA (or the source's Route Director) and a destination IP address equal to the public IP address for the Route Director of the destination (e.g., PRD 530). In step 678, the new encapsulated packet will be sent from the Route Director to the Agent for the destination device." Therefore, both the private address for the destination device and the virtual IP address for the destination are required. The combination of Leung, Forslöw, and Mehta does not teach this capability.

Fig. 7



AA/SWA Ex. 1015, p.582 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

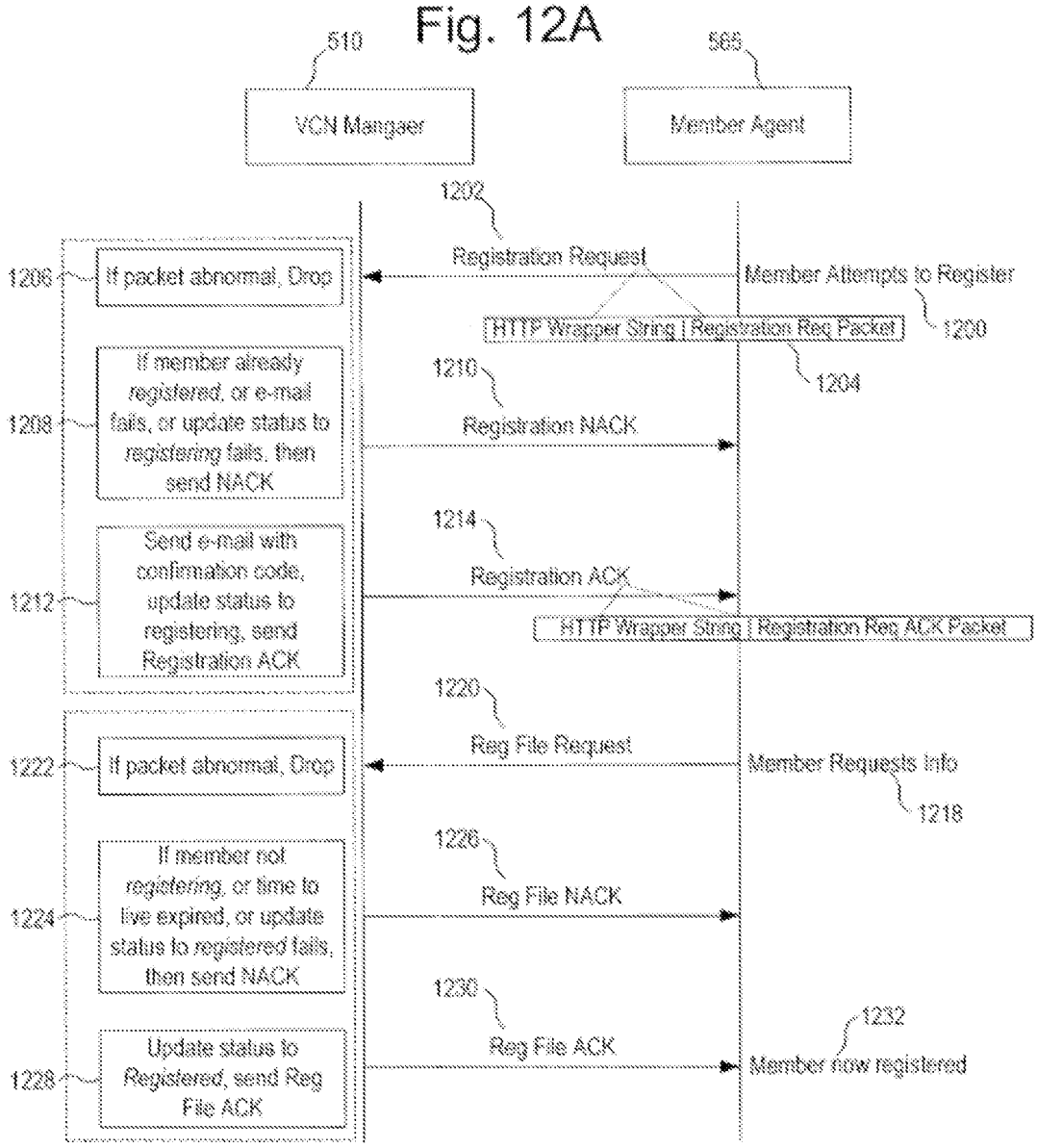
F. The combination of Leung '143, Forslöw '518, and Mehta '671 does not teach Claim 34 of the '785 Patent

53. The '785 Patent defines two distinct processes, one for registration and another for Join/Leave. The '785 Patent recites "The virtual network manager of claim 30 wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network". The specification of the '785 also defines registration as follows: "Registration in this context means registering a machine using a Member Agent or a Group Agent with the VCN Manager. Users may be required to install the Member Agent software. The link in the notification e-mail may provide the user with a location for downloading the Member Agent software as well as instructions for installing the software." … "Member Registration The registration process is the first step that a user and machine go through with the VCN Manager before becoming a member of a virtual community. There are two phases to member registration: a registration request and a registration file request. Registration happens outside of the IPsec tunnels because at registration time no IPsec tunnel exists for the user registering."

54. In this '785 Patent, the registration process is clearly explained as different from the process of Join/Leave "Member Join/Leave Once a user is registered, the user can join the VCN. Once joined, the user is a member of the VCN. Joining allows the user to let the VCN Manager and other members know that the user/member is on-line and available to communicate. The Join protocol runs between a Member Agent and the VCN Manager to establish a session key with the Manager, authenticate to the Manager, and make use of connections via the Route Directors in the community."

55. Leung does not teach registration as defined by the specification of the '785 Patent and recited in claim 34. Leung's use of the term registration and access request relates to authentication. The mentions of registration in Forslöw and Mehta are similar to Leung. Forslöw is more inspired by Mobile-IP, while Mehta views it as a cellular system registration with the carrier/operator.

Fig. 12A



AA/SWA Ex. 1015, p.585 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

IV. CONCLUSION

56. For the foregoing reasons, it is my opinion that claims 30 and 34 of the '785 Patent would not have been obvious over the prior art in the Non-Final Office Action.

57. All statements made herein of my own knowledge are true, and all statements made on information and belief are believed to be true. Further, I am aware that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.h I declare under penalty of perjury that the foregoing is true and correct.

Executed on January 8, 2025, in Boston, Massachusetts.



Dr. Guevara Noubir

AA/SWA Ex. 1015, p.586 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Curriculum Vitae

Guevara Noubir, PhD

Professor and Executive Director of Cybersecurity Programs
Northeastern University, Khoury College of Computer Sciences, Boston, MA, USA
Phone: +1 617 800 4595
Emails: g.noubir@northeastern.edu

Education:

1991-1996: Ph.D. in Computer Science.
Thesis: "Algebraic Methods for Fault-Tolerance: Applications to Communication Protocols"
Advisor: Professor Henri J. Nussbaumer
Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland

1991: MS in CS (diplôme d'ingénieur). Specialization in networks and real-time systems.
Ecole Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble (ENSIMAG) and Institut National Polytechnique de Grenoble (INPG), France.

Employment and work experience:

2011-Present:	Professor at Northeastern University – Khoury College of Computer Sciences
2019-Present:	Executive Director of Cybersecurity Programs at Northeastern University
2019-Present:	Co-Founder of Novowi
2017-Present:	Principal Investigator of Northeastern University DHS/NSA Center of Academic Excellence in Cybersecurity Research
2020-2023:	Affiliated Faculty, UM6P, Morocco
2017-2019:	Director of Cybersecurity and Information Assurance Graduate Programs
March 2017:	Distinguished Visiting Fellow, University of Edinburgh
Jul. 06-Jul. 09:	Visiting Scientist, Massachusetts Institute of Technology, LIDS.
2006-2011:	Associate Professor at Northeastern University – College of Computer and Inf. Science.
Dec. 07-Jul. 08:	Visiting Scientist, Eurecom, Sophia-Antipolis, France.
2001-2006:	Assistant Professor at Northeastern University – College of Computer and Inf. Science.
1997-2000:	Senior Research scientist (Expert) in the Real-time Software and Networking Group at the Centre Suisse d'Electronique et de Microtechnique (CSEM), Switzerland. Responsibilities: Coordinator for the workpackages of several European projects in Wireless Communications and Network Security.
Fall'1999:	Visiting Professor at University of Nebraska at Lincoln, USA.
1991-1996:	Research Assistant at the Swiss Federal Institute of Technology in Lausanne (EPFL).

External Grants:

1. "ROSETA-5G: Robust and Secure Tactical 5G Slice", Office of Naval Research (ONR), Principal Investigator, 3/2020-2/2024.
2. "Lightweight Scalable and Secure 5G and Beyond Networks", NSF Convergence Accelerator Joint NSF/DOD Track G: Securely Operating Through 5G Infrastructure, 8/2022-8/2023.
3. "RF Situational Awareness for Proactive and Dynamic Network Defense", DoD, Principal Investigator, 9/2020-8/2022.
4. "DoD CySP Capacity Building: ELastIC CYber Range (ELICCYR)", DoD, Principal Investigator with co-PI William Robertson, 9/2020-12/2021.
5. "Sensing Elasticity and Agility meet Machine Learning for Enabling Spectrum Sharing (SEAMLESS)", Defense Advanced Research Projects Agency (DARPA), PI, 1/2017-1/2020.
6. "Advancing Warfighter Technologies", ONR, co-PI with PI David Luzzi, 3/2018 – 3/2019.

AA/SWA Ex. 1015, p.587 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

7. "Analyzing, Detecting, and Mitigating Mobile Side Channel Attacks", Google Faculty Research Award, PI, 2017.
8. "Network Security Education: A Hands-On Approach", DoD/NSA, PI with Triet-V. Huu, 11/2017-10/2018.
9. "Renewal: Scholarship For Service @ Northeastern - a multi-disciplinary approach", NSF, PI with co-PIs Agnes Chan, David Kaeli, 8/2017 - 8/2023.
10. "USBRCCR: HealthSense: Assessing and Protecting Privacy in Wireless Wearable Sensor-generated Medical Data", NSF, PI, with co-PI Kaushik Chowdhury, 9/2017-8/2019.
11. "Expeditionary Cyber: Elastic Networks & Secure Localization and Synchronization", Office of Naval Research, co-PI (leading 2 out 6 projects) with PI David Luzzi, 11/2016-11/2018.
12. "EAGER: Collaborative: Towards Understanding the Attack Vector of Privacy Technologies", NSF, PI with Aziz Mohaisen (University of Buffalo), 9/2016-8/2018.
13. "Cloud Computing on Sensitive Data: Research and Education", DoD, PI with co-PI Agnes Chan, 9/2015-9/2017.
14. "TWC: Medium: Collaborative: Strengthening Wi-Fi Network Wide", National Science Foundation, Secure and Trustworthy Cyberspace, PI, 8/2014-7/2018.
15. "Multi-Disciplinary Preparation of Next Generation Information Assurance Practitioners - Renewal", NSF, PI with co-PIs Agnes Chan, David Kaeli, Wil Robertson, 9/2012-9/2018.
16. "Large-Scale Attacks in Multi-Level Interdependent Networks: Emerging Threats, Mitigation, and Recovery", Raytheon, PI.
17. "CSR: Privacy and Security for MapReduce Clouds with PASMAC", National Science Foundation, PI with Erik-Oliver Blass, 9/2012-8/2016.
18. "SWEAP - Smart Waveforms using Evasive mission-Adaptive Protocols", DARPA, PI with Agnes Chan, Rajmohan Rajaraman, and Ravi Sundaram, 5/2011 – 9/2013.
19. "Cloud Computing Security", Microsoft Research, Research Gift, 2010-2013.
20. "Workshop on Biologically Enabled Wireless Networks", National Science Foundation, PI with Bernardo Barbiellini, 9/2010-12/2012.
21. "MRI: Development of a Second-Generation Applications-Driven Wireless Sensor Networking", National Science Foundation, PI with Stefano Basagni, Peter Desnoyers, Marty Vona, 3/2010-9/2013.
22. "NeTS: A Game-Theoretic Framework for Agile and Resilient Wireless Systems", National Science Foundation, PI with Rajmohan Rajaraman, 9/2009-8/2012.
23. "EAGER: Electromagnetic Biological Transducers", National Science Foundation, Principal Investigator, 9/2009-9/2011.
24. "REU: Secure Wireless Ad Hoc Robots on Mission Autonomous-Cooperative Search and Beamforming for SWARMs", National Science Foundation, Research Experience for Undergraduates, 2009-10.
25. "CT-ISG: Secure Localization: An Education and Research Joint Approach", National Science Foundation, Principal Investigator, PI with Agnes Chan, 9/2007-8/2010.
26. "CRI: IAD Equipment for Cross-Layer Wireless Protocols Design and Prototyping", National Science Foundation, Principal Investigator, 9/2007-8/2009.
27. "SPREAD: Second-generation Protocol Resiliency Enabled through Adaptive Diversification", DARPA, PI with Ravi Sundaram, Agnes Chan, Rajmohan Rajaraman, 10/2005-12/2007.
28. "A Hands-On Course on Trustworthy Networking", Principal Investigator, Microsoft Trustworthy Computing Grant, 2006.
29. REU Supplement to NSF CAREER Award.
30. "Cross-Layer Protocols for Robust and Scalable Heterogeneous Wireless Networks", NSF CAREER Award, Principal Investigator, 2/2005-8/2010.
31. "Secure Location Related Services", DRAPER Laboratory, PI, 7/2003-6/2004.
32. "Secure Location Related Services", DRAPER Laboratory, PI, 7/2002-6/2003.
33. "Securing ATM Networks", Swisscom, PI, 1997.

Internal Grants:

"Tier 1: Institutional Data and Energy Flows: Revealing drivers of urban energy consumption through remote sensing, real-time systems data analysis, dynamic modelling, and data visualization", with Kristian Kloeckl and Matthias Ruth, 2015-2016.

"Tier 1: Secure & Robust Software Defined Radios", Northeastern University, 2013-2014.

"Secure & Robust Hybrid Wireless Networks", Northeastern University, Research and Scholarship Development Fund, Principal Investigator, July 2004 – June 2005.

Awards and Honors:

Northeastern University Excellence in Research and Creative Activity Award 2018.

Lead of DARPA Spectrum Collaboration Challenge (SC2) $1.5M winning team award in 2017, 2018, finalist 2019.

Advisor/coach of Northeastern University winning team at MITRE embedded CTF (eCTF) 2021 competition.

Advisor/coach of Northeastern University winning team of CSAW Cybersecurity Games 2020 competition.

Advisor/coach of Northeastern University winning team at MITRE embedded CTF (eCTF) 2020 competition.

Advisor/coach of Northeastern University winning team at MITRE embedded CTF (eCTF) 2019 competition.

Best paper award ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2018.

Google Faculty Research Award, 2017.

Lead of one of 4 universities funded to compete in DARPA Spectrum Collaboration Challenge (SC2).

Advised team of students in the MITRE embedded CTF (eCTF) 2017 competition, winning the "Mass Attack" achievement award given to the "most prolific offense, demonstrated by capturing significantly more flags than any other team in eCTF".

Distinguished Visitor to University of Edinburgh, "Robustness and Privacy in Mobile & Wireless Systems", March 2017.

Keynote lecture at ACM WiNTECH, "Reproducibility in Wireless Experimentation: Need, Challenges, and Approaches", October 2016.

Best Paper Award at IEEE Conference on Communications and Network Security, 2016.

Winner of DARPA Spectrum Challenge Cooperative DSC'2013 out of 90 teams ($25K Prize). Ranked 4th in DARPA Spectrum Challenge Cooperative DSC'2014.

Distinguished Lecture IEEE IAS, "LTE & LTE Security", 2013.

National Science Foundation CAREER Award (2005 – 2010).

Google Android Developers Challenge 2008, top 20 (out of over 1800 teams), won $125 award prize.

Best paper award at the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2011 (top paper out of 110), runner-up best paper award ACM WiSec'2013.

IEEE Senior Member, 2001.

Program Chair of two National Science Foundation Workshops on Biologically-Enabled Wireless Networks, and Synthetic Biology for Bio Computation and Communications 2011-2012.

Judge in the iGEM Synthetic Biology Competition – Software Division, 2012 & 2013.

Research and Education program selected for the 2009 & 2012 Highlights of the National Science Foundation Division of Computer and Network Systems.

Distinguished Lecture at University of Michigan – Dearborn, "Robustness and Privacy in Wireless Systems", November 1, 2013.

Elected member of the Dean Search Committee in the College of Computer and Information Science at Northeastern University 2012-2014.

Selected by the Provost Office for Northeastern University Research Leadership Development Initiative (ReDI), 2013-2014.

Chair of the Hiring Committee in the College of Computer and Information Science at Northeastern University 2010-2011.

AA/SWA Ex. 1015, p.589 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Invited Talks, Colloquia, and Panels:

1. Keynote lecture at IEEE Conference on Communications and Network Security (CNS), 2022.
2. Keynote lecture at ACM Conference on Security and Privacy in Wireless and Mobile Networks, "Wireless and Mobile Softwarization: Security and Privacy Pandora's Box?", 2019.
3. Keynote at the Brazilian Symposium on Information and Computational Systems Security, "Security and Privacy in Mobile and Wireless Systems", 2019.
4. Keynote lecture at ACM WiNTECH, "Reproducibility in Wireless Experimentation: Need, Challenges, and Approaches", October 2016.
5. Invited talk at MIT, "Robustness and Privacy in Mobile & Wireless Systems", February 2016.
6. Invited talk at KTH (Sweden), "Robustness and Privacy in Mobile & Wireless Systems", February 2016.
7. Invited talk at The Kostas Research Institute for Homeland Security, "Emerging Trends in Cybersecurity", March 2016.
8. Invited talk at "New Frontiers in Networking Round Table", DoD meeting, MIT, May, 2015
9. Invited talk at Worcester Polytechnic Institute "Robustness and Privacy in Wireless and Mobile Systems", April 2015.
10. Panelist at NSF Workshop on Wireless Security, March 2015.
11. DARPA Spectrum Challenge Competition, March 2014 & September 2013.
12. Distinguished Lecture at University of Michigan – Dearborn, "Robustness and Privacy in Wireless Systems", November 1, 2013.
13. Distinguished Lecture IEEE IAS Costa Rica, "LTE & LTE Security", July 2013.
14. Invited talk at UC Davis, Colloquium, "Game Theory for Wireless Adversarial Settings", March 8, 2012.
15. Invited talk at UC Irvine, Colloquium, "Wireless Networks in Cooperative and Adversarial Settings", November 18, 2011.
16. Invited talk at UT Arlington, Colloquium, "Challenges and Directions in Wireless Security", November 18, 2010.
17. Invited talk to the Intelligence Community Cyber Security Tech Exchange on Moving Target, only 5 NSF funded researchers were invited to give talks, April 2010.
18. Invited talk at UMass Lowell Colloquium, "Heterogeneous Wireless Networks in Cooperative and Adversarial Settings", November 18, 2009.
19. Invited talk at ETHZ, "Heterogeneous Wireless Networks in Cooperative and Adversarial Settings", Zurich, Switzerland, May 20, 2008.
20. Invited talk at European ICT-FORWARD initiative on emerging security threats, "Wireless Infrastructure: Emerging Threats and Countermeasures", Goteborg, Sweden, April 17, 2008.
21. Invited talk at University of Washington, "Wireless Networks in Cooperative and Adversarial Settings", May 2007.
22. "Robust Wireless Networks", invited talk to IEEE Computer Communication Workshop (CCW), 2007.
23. "Future Wireless Internet Design", invited panel talk at Wireless Internet Conference WICON'06.
24. "Scalable Secure and Robust Heterogeneous Wireless Communication" invited talk to BANANAS workshop organised by BBN Technologies, 2005.
25. "Securing Wireless Sensor Networks", invited talk to IEEE Wireless Communications and Networking Conference (WCNC) panel on sensor networks security, March 2003.
26. "Security Challenges in Multihop Wireless Ad Hoc Networks", invited talk to IEEE Symposium on Wireless Personal Multimedia Communications (WPMC) panel on security of wireless networks.
27. "Resource Management in Wireless Multihop Ad Hoc Networks", Sun Microsystems, MA, April 2001.
28. ACM SIGMETRICS invited to the panel on "The Quest for a Universal Handheld Device", Boston, July 2001.

Current Doctoral Students:

Ph.D. students, with expected year of graduation

Marinos Vomvas (MS, NTUA), 2024

Xenia Dragon (BS, Northeastern University), 2027

Stavros Dimou (MS, University Of Thessaly), 2029

AA/SWA Ex. 1015, p.590 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Graduated Doctoral Students:

Ph.D. students, with year of graduation, dissertation title, and first position upon graduation:

Norbert Ludant, "Securing Wireless Communications From the PHY Up: A Low-Layer Protocol Approach for Privacy, Security, and Resilience", 2024

Harshad Sathaye, "Towards Secure Autonomous Aerial Vehicle Navigation", 2023, ETH Zurich.

Hai Nguyen, "Robust and Secure Wireless Communications: A Deep Learning Approach", 2023, Meta.

Tien Vo-Huu, "Software Defined Radio: A Double-Edged Sword for Security and Privacy in Wireless Systems", 2022, Mathworks.

Sashank Narain, "Sensor Side-Channel Attacks on User Privacy: Analysis and Mitigation", 2018, Assistant Professor UMass Lowell.

Kenneth Block, "Covert Channels in Modern Computer Systems: The cases of Mobile and Cloud", 2018, Raytheon.

Amirali Sanatinia, "Abusing Privacy Infrastructures: Case Study of Tor", 2018.

Aldo Cassola, "Providing Privacy from the Residential Cloud", 2015, joined the faculty of Universidad San Francisco de Quito, Ecuador.

Triet Vo-Huu, "Robust Wireless Communication for Multi-Antenna, Multi-Rate, Multi-Carrier Systems", 2015, CyberFend Security; acquired by Akamai in 2017.

Koorosh Firouzbakht, "Packetized Wireless Communication Under Jamming: A Game Theoretic Approach", 2015, joined ARCON Corp.

Tao Jin, "Open Networking Infrastructure: Boosting Wireless Networks in the Era of Cloud", 2013, joined Qualcomm Research.

Hooman Javaheri, "Wireless Transfer of Energy Alongside Information: From Wireless Sensor Networks to Bio-Enabled Wireless Networks", 2012, Snap Inc.

Bishal Thapa, "Robust Wireless Communication in Adversarial Settings", 2011, BBN-Raytheon Technologies.

Yin Wang, "Distributed Diversity in Hybrid Wireless Networks", 2010, Founder of Amino Apps.

Xin Liu, "Cross Layer Design for Cooperative and Adversarial Wireless Networks", 2007, jointly advised with Ravi Sundaram, joined Microsoft Corp.

Guolong Lin, "New paradigms and approximation algorithms for optimization under uncertainty", 2006, jointly advised with Rajmohan Rajaraman, joined Akamai Technologies.

Refereed Articles

Book Chapters:

1. K. Firouzbakht, G. Noubir, M. Salehi, "Multi-Carrier Jamming Mitigation: A Proactive Game Theoretic Approach", in "Proactive and Dynamic Network Defense", Springer, 2019.
2. H. Javaheri, G. Noubir, "Wireless Transfer of Energy Alongside Information in Wireless Sensor Networks", in "Mission-Oriented Sensor Networks and Systems: Art and Science", Springer, 2019.
3. G. Noubir, "Robust Wireless Infrastructure against Jamming Attacks", in Handbook on Securing Cyber-Physical Critical Infrastructure, Morgman Kaufmann, Elsevier, 2012.
4. P. Raja, G. Noubir, "A Synchronous Model for Fieldbus Systems", in Fieldbus Technology, Ed. N. P. Mahalik, Springer, 2003.

Journal and Magazine Publications:

1. Erik-Oliver Blass and Guevara Noubir, "Forward Security with Crash Recovery for Secure Logs", ACM Transactions on Privacy and Security, 27, 1, Article 3, 2024.
2. H. N. Nguyen, M. Vomvas, T. D. Vo-Huu and G. Noubir, "WRIST: Wideband, Real-Time, Spectro-Temporal RF Identification System Using Deep Learning," in IEEE Transactions on Mobile Computing, vol. 23, no. 2, 2024.
3. M. Delamou, G. Noubir, S. Dang and E. M. Amhoud, "An Efficient OFDM-Based Monostatic Radar Design for Multitarget Detection," in IEEE Access, vol. 11, 2023.

AA/SWA Ex. 1015, p.591 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

4. L. Xin, D. Starobinski, G. Noubir, "Cascading Attacks on Wi-Fi Networks: Theory and Experiments", in Transaction on Control of Network Systems, 2020.
5. A. Vergutz, G. Noubir, M. Nogueira, "Reliability for Smart Healthcare: A Network Slicing Perspective", IEEE Networks Magazine, 2020.
6. K. Coelho, D. Damião, G. Noubir, A. Borges, M. Nogueira and J. Nacif, "Cryptographic Algorithms in Wearable Communications: An Empirical Analysis", in IEEE Communications Letters, vol. 23, no. 11, 2019.
7. T.D. Vo-Huu, E.-O. Blass, G. Noubir, "EPiC: efficient privacy-preserving counting for MapReduce", Computing 101, 1265–1286 (2019).
8. S. Narain, G. Noubir, "Mitigating Location Privacy Attacks on Mobile Devices using Dynamic App Sandboxing", in Proceedings of Privacy Enhancing Technologies Symposium (PoPETS), 2019.
9. S. Narain, T. D. Vo-Huu, K. Block and G. Noubir, "The Perils of User Tracking Using Zero-Permission Mobile Apps," in IEEE Security & Privacy, vol. 15, no. 2, pp. 32-41, March-April 2017.
10. K. Firouzbakht, G. Noubir, M. Salehi, "Linearly Constrained Bimatrix Games in Wireless Communications", IEEE Transactions on Communications, vol. 64(1), pp. 429-440, 2016.
11. E.-O Blass, T. Mayberry, G. Noubir, "Practical Forward-Secure Range and Sort Queries with Update-Oblivious Linked Lists", in Proceedings of Privacy Enhancing Technologies Symposium (PoPETS), 2015(2), pp. 81-98, De Gruyter.
12. T. Moataz, E.-O. Blass, G. Noubir, "Recursive Trees for Practical ORAM", in Proceedings of Privacy Enhancing Technologies Symposium (PoPETS), 2015(2), pp. 115-134, De Gruyter.
13. K. Firouzbakht, G. Noubir, M. Salehi, "On the Capacity of Rate-Adaptive Packetized Wireless Communication Links under Jamming", IEEE Transactions on Wireless Communications, 2014.
14. B. Zayen, A. Hayar, G. Noubir, "Game Theory-based Resource Management Strategy for Cognitive Radio Networks", Journal of Multimedia Tools and Applications, 2014.
15. A. Cassola, T. Jin, G. Noubir, B. Thapa. "Efficient Spread Spectrum Communication without Pre-shared Secrets", IEEE Transactions on Mobile Computing, 2013.
16. E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman and B. Thapa. "Performance of IEEE 802.11 under Jamming", in Mobile Networks and Applications (MONET), Springer, 2013.
17. Y. Wang, G. Noubir. "Distributed Cooperation and Diversity for Hybrid Wireless Networks", IEEE Transaction on Mobile Computing, 2013.
18. H. Javaheri, B. Barbiellini, G. Noubir. "Energy Transfer Performance of Mechanical Nanoresonators Coupled with Electromagnetic Fields", Nanoscale Research Letters 2012.
19. B. Zayen, A. Hayar and G. Noubir, "Game Theory-Based Resource Management Strategy for Cognitive Radio Networks", Journal of Multimedia Tools and Applications, 2012.
20. Erik-Oliver Blass, Anil Kurmus, Refik Molva, Guevara Noubir, Abdullatif Shikfa, "The Ff-family of protocols for RFID-privacy and authentication", in IEEE Transactions on Dependable and Secure Computing, 2011.
21. G. Noubir, B. Thapa, Y. Wang, "Experimentation-Oriented Platform for Development and Evaluation of MANET Cross-Layer Protocols", in Ad Hoc Networks Journal, Elsevier, May, 2008.
22. G. Lin, G. Noubir, "On Link Layer Denial of Service in DATA Wireless LANs", in the Wiley Journal on Wireless Communications and Mobile Computing, Wiley, August, 2004.
23. S. Ci, H. Sharif, and G. Noubir. "Improving Goodput of the IEEE 802.11 MAC Protocol by Using Congestion Control Methods", in the International Journal on Wireless and Optical Communications (IJWOC), Vol. 1, No.2 (2004) 1-9, World Scientific Publishing.
24. G. Noubir, G. Lin (2003). "Low Power DoS Attacks in Data Wireless LANs and Countermeasures", in ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), volume 7, Issue 3.
25. G. Noubir, G. Lin, M. Golitsine, N. Plante (2003). "Secure Sharing of Location Information over Ad Hoc Networks: An Application of Secure Multicast", in ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), volume 7, Issue 3.
26. G. Noubir, K. Vijayanada and H. J. Nussbaumer (1998). "Signature-Based Method for Run-Time Fault Detection in Communication Protocols." Computer Communications Journal, Butterworth-Heinemann, Vol.21, No 5, May 1998.
27. G. Noubir and H. J. Nussbaumer (1995). "Self-correcting polynomial programs." In Journal of Reliable Computing, Vol 2, No 2, 1996.
28. P. Raja and G. Noubir (1993). "Static and dynamic polling mechanisms for fieldbus networks." In the

AA/SWA Ex. 1015, p.592 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Operating Systems Review, 27(3), pages 34-45.
29. P. Raja, G. Noubir, L. Ruiz, J. Hernandez, and J.-D. Decotignie (1993). "Analysis of polling protocols for fieldbus networks." In the ACM-SIGCOMM Computer Communication Review, 23(3):69--90.

Conference publications:

1. N. Ludant, P. Robyns and G. Noubir, "From 5G Sniffing to Harvesting Leakages of Privacy-Preserving Messengers", in IEEE Symposium on Security and Privacy, 2023.
2. Hai N. Nguyen and Guevara Noubir, "JaX: Detecting and Cancelling High-power Jammers Using Convolutional Neural Network", ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'23), 2023.
3. H. Sathaye, G. Noubir, and A. Ranganathan, "On the Implications of Spoofing and Jamming Aviation Datalink Applications", in the Annual Computer Security Applications Conference (ACSAC), 2022.
4. H. N. Nguyen, G. Noubir, "Universal Beamforming: A Deep RFML Approach", in ACM International Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 2022.
5. Tim Upthegrove, Guevara Noubir, Bishal Thapa, Dan Smith, Colin Funai, Scott Loos, Greg Kuperman, "Rapid Interoperability with OverlAI Gateways," MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM), 2022.
6. N. Ludant, T. D. Vo-Huu, S. Narain, G. Noubir, "Linking Bluetooth LE & Classic and Implications for Privacy-Preserving Bluetooth-Based Protocols", in IEEE Symposium on Security and Privacy, 2021.
7. D. Giese, G. Noubir, "Amazon echo dot or the reverberating secrets of IoT devices", in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'21), 2021, **Runner-Up Best Paper Award**.
8. N. Ludant, G. Noubir, "SigUnder: a stealthy 5G low power attack and defenses", in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'21), 2021.
9. M. Vomvas, E.-O. Blass, G. Noubir, "SELEST: secure elevation estimation of drones using MPC", in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'21), 2021.
10. T. D. Vo-Huu, T. D. Vo-Huu, G. Noubir, "Spectrum-flexible secure broadcast ranging", in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'21), 2021.
11. H. Nguyen, M. Vomvas, T. D. Vo-Huu, G. Noubir, "Spectro-Temporal RF Identification using Deep Learning", in Proceedings of the ACM International Symposium on Mobility Management and Wireless Access (MobiWac'21), 2021.
12. Tien D. Vo-Huu, Norbert Ludant, Triet D. Vo-Huu, "Pilotless FS-FBMC for Flexible Spectrum Access and Sharing", IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN'21), 2021.
13. K. Zerhouni, E. M. Amhoud and G. Noubir, "Deep Neural Networks for Multicarrier Waveforms Classification in UAV Networks," 2021 17th International Symposium on Wireless Communication Systems (ISWCS), 2021.
14. M. J. Idrissi, I. Berrada and G. Noubir, "FEDBS: Learning on Non-IID Data in Federated Learning using Batch Normalization," in IEEE International Conference on Tools with Artificial Intelligence (ICTAI), 2021.
15. M. Cominelli, F. Gringoli, M. Lind, P. Patras, G. Noubir, "Even Black Cats Cannot Stay Hidden in the Dark: Full-band De-anonymization of Bluetooth Classic Devices", IEEE Symposium on Security and Privacy, 2020.
16. P. Robyns, M. M. Di Martino, P. Quax, W. Lamotte, G. Noubir, "Practical Operation Extraction from Electromagnetic Leakage for Side-Channel Analysis and Reverse Engineering", ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2020.
17. H. Sathaye, A. Ranganathan, G. Noubir, "Wireless Attacks on Aircraft Instrument Landing Systems", Usenix Security Symposium, 2019.
18. M. Stute, S. Narain, A. Mariotto, A. Heinrich, G. Noubir, M. Hollick, "A Billion Open Houses for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link", Usenix Security Symposium, 2019.
19. S. Narain, A. Ranganathan, G. Noubir, "Security of GPS/INS based On-road Location Tracking Systems", IEEE Symposium on Security and Privacy, 2019.
20. A. Aminian, G. Noubir, "Deep Cross-Modal Age Estimation", in Proceedings of Computer Vision Conference (CVC), Springer, 2019.

21. Kenneth Block and Guevara Noubir, "My Magnetometer Is Telling You Where I've Been?: A Mobile Device Permissionless Location Attack", in ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '18), **Best Paper Award**.
22. K. Block, S. Narain, G. Noubir, "An Autonomic and Permissionless Android Covert Channel", ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2017.
23. E.-O. Blass, T. Mayberry and G. Noubir, "Multi-Client Oblivious RAM Secure Against Malicious Servers", International Conference on Applied Cryptography and Network Security (ACNS), 2017.
24. E.-O. Blass, G. Noubir, "Secure Logging with Crash Tolerance", IEEE Conference on Communications and Networks Security (CNS), 2017.
25. A. Sanatinia et al., "Hyperdrive: A flexible cloud testbed for research and education", IEEE International Symposium on Technologies for Homeland Security (HST), 2017.
26. S. Narain, T. Vo-Huu, K. Block, and G. Noubir, "Inferring Location and Traffic Patterns without Permissions using Side-Channels", in Proceedings of IEEE Symposium on Security & Privacy, 2016.
27. T. Vo-Huu, T. Vo-Huu, G. Noubir, "Fingerprinting Wi-Fi Devices using Software Defined Radio", in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2016.
28. T. Vo-Huu, T. Vo-Huu, G. Noubir, "Interleaving Jamming in Wi-Fi Networks", in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2016.
29. A. Sanatinia, G. Noubir, "Honey Onions: a Framework for Characterizing and Identifying Misbehaving Tor HSDirs", in Proceedings of IEEE Conference on Communication Networks Security, 2016.
30. G. Noubir, M. Médard, P. Chin, "Wi (deband)-Fi: A Proposal for an Opportunistic Wideband Architecture based on Wi-Fi", Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access, 2016.
31. A. Sanatinia, G. Noubir, "HOnions: Towards Detection and Identification of Misbehaving Tor HSDirs", Hot PETS (part of the PETS Symposium), 2016.
32. Liangxiao Xin, D. Starobinski, G. Noubir, "Cascading Denial of Service Attacks on Wi-Fi Networks", in Proceedings of IEEE Conference on Communication Networks Security, 2016, **Best Paper Award**.
33. G. Noubir, M. Medard, P. Chin, "Wi (deband)-Fi: A Proposal for an Opportunistic Wideband Architecture based on Wi-Fi", Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access.
34. Guevara Noubir, Amirali Sanatinia, "Trusted code execution on untrusted platforms using Intel SGX", Virus Bulletin, 2016.
35. G. Noubir, A. Sanatinia, "Honey Onions: Exposing snooping tor HSDir relays", DEF CON 24, 2016.
36. A. Cassola, E.-O. Blass, and G. Noubir, "Authenticating Privately over Public Wi-Fi Hotspots", in Proceedings of the ACM Conference on Computer and Communications Security (CCS'15), acceptance rate 19% (128/660).
37. E.-O Blass, T. Mayberry, G. Noubir, "Practical Forward-Secure Range and Sort Queries with Update-Oblivious Linked Lists", in Proceedings of Privacy Enhancing Technologies Symposium (PETS'15), 2015.
38. T. Moataz, E.-O. Blass, G. Noubir, "Recursive Trees for Practical ORAM", in Proceedings of Privacy Enhancing Technologies Symposium (PETS'15), 2015.
39. A. Sanatinia, G. Noubir, "OnionBots: Subverting Privacy Infrastructure for Cyber Attacks", in Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks, 2015 acceptance rate 21% (50/229).
40. T. Vo-Huu, G. Noubir, "Mitigating Rate Attacks through Crypto-Coded Modulation", in Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2015, acceptance rate 14% (37/250).
41. E.-O. Blass, T. Mayberry, G. Noubir, K. Onarlioglu, "Toward Robust Hidden Volumes using Write-Only Oblivious RAM", in Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2014, acceptance rate 19% (114/585).
42. S. Narain, A. Sanatinia, G. Noubir, "Single-stroke Language-Agnostic Keylogging using Stereo-Microphones and Domain Specific Machine Learning", in Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Network, Wisec'14, 2014, acceptance rate full papers 15% (14/96).
43. K. Firouzbakht, G. Noubir, M. Salehi, "Packetized wireless communication under jamming, a constrained bimatrix game", in IEEE GLOBECOM 2014.

AA/SWA Ex. 1015, p.594 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

44. T. Vo-Huu, E.-O. Blass, G. Noubir, "Counter-Jamming using Mixed Mechanical and Software Interference Cancellation", in Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Network, Wisec'13, 2013, acceptance rate full papers 14% (11/76), **Runner-up Best Paper Award**.
45. A. Cassola, W. Robertson, E. Kirda, G. Noubir. "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication", in the Proceedings of the Network & Distributed System Security Symposium, NDSS, 2013, acceptance rate 17% (46/258).
46. Z. A. Qazi, J.K. Lee, T. Jin, G. Bellala, M. Arndt, G. Noubir, "Application-awareness in SDN", In Proceedings of ACM SIGCOMM, Demo, 2013.
47. K. Firouzbakht, G. Noubir, M. Salehi, "On the performance of multi-layer superposition coding scheme under constrained jamming", in Proceedings of the 47th IEEE Annual Conference on Information Sciences and Systems, CISS'2013.
48. K. Firouzbakht, G. Noubir, M. Salehi, "On the Capacity of Rate-Adaptive Packetized Wireless Communication Links under Jamming", in Proceedings of ACM Conference on Wireless Network Security, Wisec'12, acceptance rate 22% (17/76).
49. G. Noubir, R. Rajaraman, B. Sheng, B. Thapa, "On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming", in Proceedings of ACM Conference on Wireless Network Security, Wisec'11, **Best Paper Award,** acceptance rate full papers 11% (10/91).
50. J. Tao, G. Noubir, B. Sheng, "WiZi-Cloud: Application-transparent Dual ZigBee-WiFi Radios for Low Power Internet Access", in Proceedings of IEEE Infocom 2011, acceptance rate 15% (291/1823).
51. K. Firouzbakht, G. Noubir, M. Salehi, "Superposition coding in an adversarial environment", Annual Conference on Information Sciences and Systems, CISS 2011.
52. B. Zayen, A. Hayar and G. Noubir, "Utility/Pricing-based Resource Allocation Strategy for Cognitive Radio Systems", ICMCS'11, 2nd International Conference on Multimedia Computing and Systems, 2011.
53. H. Javaheri, G. Noubir, Y. Wang, "Distributed Cooperation and Diversity for Hybrid Wireless Networks", in Proceedings of WWIC, 2010, LNCS, Springer-Verlag.
54. H. Javaheri, G. Noubir, "iPoint: A Platform-Independent Passive Information Kiosk for Cell Phones", in Proceedings of IEEE SECON, 2010, acceptance rate 20% (63/309).
55. T. Jin, G. Noubir, B. Thapa, "Zero Pre-shared Secret Key Establishment in Presence of Jammers", in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc, 2009, acceptance rate 17% (31/175).
56. H. Javaheri, G. Noubir, S. Noubir (2009). "RF Control of Biological Systems: Applications to Wireless Sensor Networks", in Proceedings of the Fourth International Conference on Nano-Networks, NanoNet'09, LNCS, Springer-Verlag.
57. E. Bayrataroglu, C. King, X. Liu, G. Noubir, and B. Thapa (2008). "On the Performance of IEEE 802.11 under Jamming", in Proceedings of IEEE Infocom 2008, acceptance rate 20% (236/1160).
58. P. Tague, D. Slater, G. Noubir, R. Poovendran (2008). "Linear Programming Models for Jamming Attacks on Network Traffic Flows", 6th Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'08), April 2008.
59. Agnes Chan, Xin Liu, Guevara Noubir, and Bishal Thapa (2007), "Control Channel Jamming: Resilience and Identification of Traitors", IEEE International Symposium on Information Theory ISIT'07.
60. H. Javaheri, G. Noubir, Y. Wang (2007). "Cross-Layer distributed diversity for heterogeneous wireless networks", in Proceedings of the Fifth International Conference on Wired/Wireless Internet Communication, WWIC'07, LNCS, Springer-Verlag, Portugal, May 2007.
61. Xin Liu, Guevara Noubir, Ravi Sundaram, San Tan (2007). "SPREAD: Foiling Smart Jammers using Multi-layer Agility", IEEE Infocom'07 Mini-Symposium.
62. G. Noubir (2006). "SWARM: Secure Wireless Ad hoc Robots on Mission - A Course Where Wireless Security Meets Robotics", in the Proceedings of The Colloquium for Information Systems Security Education, CISSE'06.
63. L. Jia, G. Noubir, R. Rajaraman, and R. Sundaram. "Group-independent Spanning Tree for Data Aggregation in Dense Sensor Networks," in Proceedings of IEEE DCOSS 2006.
64. Ch. Ravi Chandra, A. Kumarasubramaniam, R. Manokaran, G. Noubir and C. Pandu Rangan, and R. Sundaram. "Steganographic Communication in Ordered Channels", in Proceedings of Information Hiding IH 2006.

AA/SWA Ex. 1015, p.595 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

65. L. Jia, G. Lin, G. Noubir, R. Rajaraman and R. Sundaram (2005), "Universal Approximations for TSP, Steiner Tree and Set Cover", in Proceedings of ACM STOC'05.
66. J. Chen, L. Jia, X. Liu, G. Noubir, R. Sundaram (2005). "Minimum Energy Accumulative Routing in Wireless Networks", in Proceedings of IEEE Infocom.
67. T. Kaya, P. Lin, G. Noubir, and W. Qian (2005). "Efficient Multicast Trees with Local Knowledge on Wireless Ad hoc Networks" in the proceedings of the International Conference on Wired/Wireless Internet Communications, Lecture Notes in Computer Science, Springer-Verlag, 2005.
68. L. Jia, X. Liu, G. Noubir, R. Rajaraman (2005). "Transmission Power Control for Ad Hoc Wireless Networks: Throughput, Energy and Fairness", in Proceedings of IEEE Wireless Communications on Networking Conference, WCNC'05.
69. G. Lin, G. Noubir, R. Rajaraman (2004). "Mobility Models for Ad hoc Network Simulation", IEEE Infocom'04.
70. G. Noubir (2004). "On Connectivity in Ad Hoc Network under Jamming Using Directional Antennas and Mobility", in International Conference on Wired /Wireless Internet Communications, Lecture Notes in Computer Science, Springer-Verlag, WWIC'04.
71. F. Zhu, A. Chan, G. Noubir (2003). "Optimal Tree Structure for Key Management of Simultaneous Join/Leave in Secure Multicast", in Proceedings of MILCOM'03.
72. T. Kaya, G. Lin, G. Noubir, A. Yilmaz (2003). "Secure Multicast Groups on Ad Hoc Networks", in Proceedings of ACM Workshop on Security of Ad hoc and Sensor Networks, SASN'03.
73. G. Noubir, G. Lin, M. Golitsine, N. Plante (2003). "Secure Sharing of Location Information over Ad Hoc Networks: An Application of Secure Multicast", Poster, ACM Mobihoc, 2003.
74. G. Noubir, G. Lin (2003). "Low Power DoS Attacks in Data Wireless LANs and Countermeasures", Poster, ACM Mobihoc.
75. G. Lin, G. Noubir (2003). "Secure Multicast over Multihop Wireless Ad Hoc Networks", in the Proceedings of Mobile Ad Hoc Networks Workshop (MADNET), Sophia-Antipolis, France.
76. G. Lin, G. Noubir (2002). "Energy Efficient Broadcast with Sectored Antennas in Wireless Ad Hoc Networks", in Proceedings of IASTED/IEEE Wireless and Optical Communications Conference.
77. G. Noubir, F. Zhu, A. H. Chan (2002). "Key Management for Simultaneous Join/Leave in Secure Multicast", to appear in the Proceedings of IEEE International Symposium on Information Theory (ISIT).
78. J.-C. Birget, X. Zou, G. Noubir, B. Ramamurthy, "Hierarchy-Based Access Control in Distributed Environments" in the Proceedings of IEEE ICC, June 2001.
79. S. Ci, H. Sharif, and G. Noubir (2001). "Improving the Performance of the MAC Layer Using Congestion Control/Avoidance Methods in a Wireless Network" in the Proceedings of the 16th ACM Symposium on Applied Computing, Las Vegas, 2001.
80. G. Noubir, and L. von Allmen (1999), "Security Issues in Internet Protocols over Satellite Links", In Proceedings of the IEEE Vehicular Technology Conference (VTC'99), Amsterdam, Holland.
81. G. Noubir (1999). "A Scalable Key Distribution Scheme for Dynamic Multicast Groups." In Proceedings of the Third European Research Seminar on Advances in Distributed Systems, Madeira Island, Portugal
82. G. Noubir (1999). "FRAMES Demonstrator Packet Access Mode." In Proceedings of the ACTS FRAMES Workshop, Delft, Netherlands.
83. G. Noubir (1998). "Inter-layer Radio Resource Management in Hierarchical Cell Structures for the FRAMES Project." In Proceedings of the IEEE Globecom98, Sydney, Australia.
84. G. Noubir (1998). "Collision-Free One-Way Communication Using Reed-Solomon Codes." In Proceedings of the IEEE International Symposium on Information Theory and Applications (ISITA'98), Mexico city.
85. G. Noubir (1998). "Inter-layer Radio Resource Management in Hierarchical Cell Structures." In Proceedings of the 9th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'98), Boston, Massachusetts.
86. B. Y. Choueiry and G. Noubir (1998). "On the computation of Local Interchangeability in Discrete Constraint Satisfaction Problems." In the Proceedings of AAAI'98, pages 326-333. Madison, Wisconsin.
87. B. Y. Choueiry and G. Noubir (1997). "Using Complete No-Good Sets to Build a Disjunctive Decomposition Scheme for Discrete Constraints Satisfaction Problems." In the Proceedings of the 10th International FLAIRS Conference, pages 40-46. Daytona Beach, Fla.
88. Noubir, B. Y. Choueiry and H. J. Nussbaumer (1996). "Fault Tolerant Multiple Observers Using Error Control

AA/SWA Ex. 1015, p.596 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Codes." In Proceedings of the IEEE International Conference on Network Protocols ICNP'96, Ohio, U.S.A.
89. G. Noubir and B. Y. Choueiry (1996). "Algebraic Techniques for the Optimization of Control Flow Checking." In the Proceedings of the 26th IEEE Symposium on Fault-Tolerant Computing (FTCS'96) pages 128-137, Sendai, Japan.
90. G. Noubir and M.-A. Péraldi (1996). "Vérification de la Sureté d'Exécution de Grafcets." In Real-Time Systems and Embeded Systems, RTS'96. Paris, France, January, 1996.
91. B. Y. Choueiry, G. Noubir, and B. Faltings (1996). "Blending AI and mathematics: the case of resource allocation." In the Proceedings of the Fourth International Symposium on Artificial Intelligence and Mathematics. Fort Lauderdale, Fla.
92. G. Noubir, K. Vijayananda, and H. J. Nussbaumer (1995). "A robust transport protocol for run-time fault detection." In Proceedings of ICNP'95: IEEE International Conference on Network Protocols, Tokyo, Japan.
93. G. Noubir and H. J. Nussbaumer (1995). "Voting with low communication overhead." In Proceedings of the Sixth International Conference on Signal Processing Applications & Technology (ICSPAT`95), Boston, MA.
94. G. Noubir and H. J. Nussbaumer (1995). "Self-correcting polynomial programs." In Proceedings of Symposium of Scientific Computing, Computer Arithmetic & Validated Numerics, Kluwer-verlag.
95. G. Noubir, K. Vijayananda, and P. Raja (1995). "Signature based technique for fault detection in communication protocols." In Proceedings of IEEE International Symposium on Information Theory.
96. G. Noubir, K. Vijayananda, and G. Berthet (1995). "Robust communication protocols for run-time fault detection." In Proceedings of the Twelfth IEEE International Conference on Computer Communication (ICCC`95), pages 493-498. Seoul, Korea.
97. G. Noubir and K. Vijayananda (1995). "Fault detection in communication protocols using signature analysis." In Proceedings of the International Conference on Intelligent Information Management Systems (IASTED/ISMM'95), pages 148-151. Washington, D.C.
98. G. Noubir and H. J. Nussbaumer (1995). "Arithmetization and self-reducibility methods for fault-detection in combinatorial circuits." In Proceedings of the Thirteenth IASTED International Conference Applied Informatics, pages: 21-23. Innsbruck, Austria.
99. G. Berthet, K. Vijayananda, and G. Noubir (1995). "A new presentation layer protocol for partitioned syntax transformation model." In Proceedings of the IEEE Twelfth International Conference on Computer Communication (ICCC'95), pages 499-504. Seoul, Korea.
100. T. Kouthon, G. Noubir, P. Raja, and J.-D. Decotignie (1995). "Modeling distributed PLC control." In Proceedings of the IFAC/IFIP Workshop on Algorithms and Architectures for Real-Time Control.
101. G. Noubir, Prasad Raja, and J.-D. Decotignie (1994). "Simulating the fieldbus synchronous model by timed Petri nets." In Proceedings of IEEE IECON'94, pages 1205-1210. Bologna, Italy.
102. D. R. Stephens, G. Noubir, and M. Moreaux (1994). "Tool path correction in 2 and 3 dimensions." In Proceedings of EURISCON'94, pages 1796-1809. Malaga, Spain.
103. B. Y. Choueiry, B. Faltings, and G. Noubir (1994). "Abstraction methods for resource allocation." In Proceedings 1994 Workshop on Theory Reformulation and Abstraction, pages 2-70/2-90.
104. G. Noubir, Daniel R. Stephens, and Prasad Raja (1993). "Specification of timed finite state machine in Z for distributed real-time systems.". In Proceedings of the IEEE Fourth Workshop on Future Trends in Distributed Computing Systems, pages 319-325. Lisbon, Portugal.
105. P. Raja, G. Noubir, L. Ruiz, J. Hernandez, and J.-D. Decotignie (1993). "Synchronous model for distributed real-time control systems." In Proceedings ICPADS'93, pages 26-30. Taipei, Taiwan.
106. P. Raja, J. Hernandez, L. Ruiz, G. Noubir, and J.-D. Decotignie (1993). "A software architecture for maintaining temporal consistency in a distributed real-time environment." In Proceedings of COMPSAC'93, pages 380-387. Phoenix, Arizona.
107. P. Raja and G. Noubir (1993). "Implementing synchronous network model on a FIP network." In IEEE Workshop on Advances in Parallel Distributed Systems (in conjunction with IEEE Symposium on reliable Distributed Systems), pages 20-27. Princeton, NJ.
108. P. Raja and G. Noubir (1993). "A functional approach for expressing temporal properties in inputs and outputs of real-time applications." In Proceedings of the Fourth Workshop on Future Trends in Distributed Computing Systems, pages 312-338. Lisbon, Portugal.
109. P. Raja, G. Noubir, L. Ruiz, J. Hernandez, M. Riese, and J.-D. Decotignie (1993). "Analysis of a class of polling protocols for fieldbus networks." In Proceedings of ICDDS'93, pages 139-155, Spain.

AA/SWA Ex. 1015, p.597 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Patents

1. Erik-Oliver Blass, Guevara Noubir, "Plaintext equivalence proof techniques in communication systems", US20190109712A1, filed 2018.
2. Erik-Oliver Blass, Guevara Noubir, "Secure and Encrypted Logging Systems and Methods with Data Recovery", filed 2019.

AA/SWA Ex. 1015, p.598 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Courses at Northeastern University:

	Quarter Courses	Quarter
COM3510	Computer Networks (new prep)	W'01
COM3525	Wireless Networks (new course)	S'01
COM3515	Internet-working (new prep)	F'01
COM3525	Wireless Networks	W'02
COM1337	UG-Computer Networks (new prep)	S'02
COM3510	Computer Networks	F'02
COM3522	Network Security (new course)	W'03
COM3525	Wireless Networks	S'03
	Semester Courses	**Semester**
CSG150	Fundamentals of Networking	F'03
CSG254	Network Security (new course)	S'04
CSG252	Cryptography (new prep)	F'04
CSG254	Network Security	S'05
CSG252	Cryptography	F'05
CSG254	Network Security	S'06
CSU610	Senior Honor Seminar (Secure Wireless Ad hoc Robots on Mission - SWARM)	S'06
CSG254	Network Security	S'07
CSU610	Senior Honor Seminar (SWARM)	S'07
CSG254	Network Security	S'09
CSG258	SWARM I	S'09
CS6740/4740	Network Security	F'09
CS6740/4740	Network Security	S'10
CS5700/4700	Fundamentals of Computer Networks	S'10
CS6740/4740	Network Security	F'10
CS7780	Special Topics in Networks	S'11
CS5700/4700	Fundamentals of Computer Networks	F'11
CS6710	Wireless Networks	S'12
CS5700/4700	Fundamentals of Computer Networks	S'12
CS6740/4740	Network Security	F'12
CS6740/4740	Network Security	S'13
CS6740/4740	Network Security	F'13
CS6740/4740	Network Security	S'14
CS7780	Special Topics: Wireless Security	F'14
CS6740/4740	Network Security	F'15
CS6710	Mobile and Wireless Systems	S'16
CS8674	Deconstructing the Cloud: a Security Perspective	S'16
CS6740/4740	Network Security	F'16
CS6740/4740	Network Security	S'17
CS6740/4740	Network Security	F'17
CS6740/4740	Network Security	F'18
IA 8660	INSuRE: Research Projects in National Information Security	F'18
CS6740/4740	Network Security	F'19
CY4930	Capstone in Cybersecurity	S'20
CY6740/4740	Network Security	F'22
CY6740/4740	Network Security	S'24

AA/SWA Ex. 1015, p.599 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Courses prior to joining Northeastern University:

CSCE990: "Advanced Topics in Mobile and Wireless Networking", University of Nebraska at Lincoln, F'99.
CSCE463/863: "Introduction to Coding Theory", University of Nebraska at Lincoln, F'99.
Doctoral course: "Probabilistic and Interactive Algorithms", with Professor Henri J. Nussbaumer at EPFL, 1993.

AA/SWA Ex. 1015, p.600 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Service to the Profession:

Associate Editor of ACM Transactions of Privacy and Security (2016 – 2020)
Associate Editor of IEEE Transaction on Mobile Computing (2012 – 2018).
Associate Editor of ACM Transactions of Information Forensics and Security (2016 – 2018)
Associate Editor of ACM Transactions of Information and System Security (2014 – 2016)
Area Editor of Elsevier Computer Networks Journal (2012 - 2017).

Steering Committee of ACM Security and Privacy in Wireless and Mobile Networks (WiSec) 2018 – 2024.

General Chair ACM Security and Privacy in Wireless and Mobile Networks (WiSec) 2017.

TPC co-chair of IEEE Conference on Distributed Computing in Sensor Systems (DCOSS) 2018.
TPC co-chair of ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2015.
TPC co-chair of IEEE Conference on Communications and Network Security (CNS) 2015.
TPC co-chair of IEEE International Symposium World of Wireless Mobile and Multimedia Networks (WoWMoM) 2015.
TPC co-chair of IEEE Conference on Sensing, Communication, and Networking (SECON) 2014.
TPC co-chair of the International Conference on Networked Systems (NETYS) 2014 (LNCS 8593).
TPC co-Chair International Conference on Computer Communication Networks 2012.
TPC co-Chair IEEE Workshop on Data Security and PrivAcy in wireless Networks D-SPAN 2011-2012.

Judge in the iGEM Synthetic Biology Competition – Software Division, 2012 & 2013.

Member of Technical Program Committee of Conferences:

ACM Wireless Security Conference WiSec 2012-2024.
IEEE Symposium on Security and Privacy 2021-2025.
Usenix Security 2020-2021.
Area Chair IEEE Conference on Communications and Network Security (CNS) 2016-2017.
AsiaCCS 2015-2017.
Program Committee Privacy Enhancing Technologies Symposium (PETS 2016-2017), Editorial Board of PoPETS 2016-2017.
IEEE Infocom 2008-2012, 2016.
International Conference on Mobile Computing and Networking MobiCom 2016, 2015, 2009, 2007.
International Conference on Security and Cryptography (SECRYPT) 2012.
International Symposium on Mobile Ad Hoc Networking and Computing MobiHoc'07.
International Wired/Wireless Internet Communications WWIC'04-WWIC'11 (LNCS).
International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, WiOpt'06, WiOpt'07.
International Symposium on Stabilization, Safety, and Security of Distributed Systems SSS'08-12.
IEEE Symposium on Network Security and Information Assurance (part of ICC'06).
International Conference on Information and Communications Security ICICS'04 (LNCS 3269).

I have served as a reviewer for the following funding agencies:

I was invited to serve on over 40 National Science Foundation panels to review proposals on Wireless Networking and Network Security (2002-) [reviewed hundreds of proposals].

I was also invited to review proposals for the French academic research program on computer security and dependability (ACISI), Israel Science Foundation, Hong Kong Research Grants Council, and Qatar National Research Fund.

External evaluator of the Computer Science Department of University of Massachusetts Boston (Academic Quality Assessment and Development – AQUAD), 2015.

AA/SWA Ex. 1015, p.601 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Ph.D. committees:

Konstantinos Athanasiou (Advisor Professor T. Wahl)
Milan Stute (Advisor Professor M. Hollick, 2020)
Matthias Schulz (Advisor Professor M. Hollick, 2018)
Eric Miles (Advisor Professor E. Viola, 2014)
Abhishek Samanta (Advisor Professor R. Sundaram, 2014)
Peter Golbus (Advisor Professor J. Aslam, 2014)
Dimitrios Kanoulakis (Advisor Professor M. Vona, 2014)
Abdulla Al-Ali (ECE, Advisor Professor K. Chowdhury, 2014)
Ruopeng Ye (Advisor Professor A. Chan 2008)
Feng Zhu (Advisor Professor A. Chan 2007)
Michele Battelli (ECE, Advisor: Professor S. Basagni 2007).
Lujun Jia (Advisor: Professor R. Rajaraman, 2005).
Rituparna Ghosh (ECE, Advisor: Professor S. Basagni, 2005).
Yue Fang (ECE, Advisor Professor B. McDonald, 2005).
Victor Grinberg (Advisor: Professor G. Cooperman, 2001).
Ducan Shek Wong (Advisor: Professor A. Chan, 2001).

Industry Collaboration:

Airbus, BAE Systems, BBN Technologies, Draper Labs, Google, Microsoft, Raytheon.

AA/SWA Ex. 1015, p.602 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/019,519	**01/08/2025 07:41:19 PM Z ET**	**IVIPR-RE90019519**

Title of Invention

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	7949785
CONFIRMATION #	2698	FILED BY	Heather King
PATENT CENTER #	68658386	FILING DATE	05/22/2024
CUSTOMER #	3624	FIRST NAMED INVENTOR	- 7949785
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brandon Theiss

Documents

TOTAL DOCUMENTS: 10

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
IVIPR_RE90019519_Ex2002_PC.pdf		6	Non Patent Literature	1504 KB
IVIPR_RE90019519_Ex2003_PC.pdf		34	Non Patent Literature	2023 KB
IVIPR_RE90019519_Ex2004_PC.pdf		8	Non Patent Literature	9878 KB
IVIPR_RE90019519_Ex2005_PC.pdf		39	Non Patent Literature	199 KB
IVIPR_RE90019519_ResponsetoNFOA_PC.pdf		29	-	328 KB
IVIPR_RE90019519_ResponsetoNFOA_PC-XI.A....pdf	(1-28)	28	Response after non-final action-owner timely	324 KB
IVIPR_RE90019519_Respo	(29-29)	1	Reexam Certificate of Service	62 KB

nsetoNFOA_PC-RXC/SR.pdf			
IVIPR_RE90019519_DeclarationEx2001_PC.pdf	45	Affidavit-not covered under specific rule	2287 KB
IVIPR_RE90019519_Ex2006_PC.pdf	4	Non Patent Literature	2463 KB
IVIPR_RE90019519_Ex2008_PC.pdf	7	Non Patent Literature	2250 KB
IVIPR_RE90019519_Ex2007_PC.pdf	55	Non Patent Literature	15987 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
IVIPR_RE90019519_Ex2002_PC.pdf	4BD33A84994B414D25E6D47276044F595056AADDAAA4DCDD9188B0968A8FFC413566930B3CF08F55D095F8BE9B05682E931BCE410E2AA3A3230927A852D9DB97
IVIPR_RE90019519_Ex2003_PC.pdf	3977CDE9A865FD66332A0234F78D4E69C6ED6672B824D96859B8697DC4C35ADF019E575003C8672F4F990E77F3D2A1A48B3AE49AF9E27EAA75A6187047CF01B1
IVIPR_RE90019519_Ex2004_PC.pdf	2748B5E4AAF7B99C171407077B365170316071D1A95FCB0FEB6DDAABCCA67683003BDD59D8128C248F52265EC2B8740A8FC94293E26EE1217A0AB146B349416E
IVIPR_RE90019519_Ex2005_PC.pdf	3DE806D9F3909D2C0177BDCE5866B1259FF94046C3B71E5328E53FDE925283E28FC246D79C799594597C2E8DF044369B060673E49A456298FA970D53D08E7BF9
IVIPR_RE90019519_ResponsetoNFOA_PC.pdf	E3E191B8FBC8409DC293309961D6F84557E08D362F90F307F9355A258625D80644A89E3D5354BBB93008E4ED99AD65363A3635B7C239E4A6F9B75F7427ABFB53
IVIPR_RE90019519_ResponsetoNFOA_PC-XI.A....pdf	8C5AE81F1AF2D6175EFC3A9D63BBBFC9601C11A54E254752AEE1A6BE242B0540E83035C88B409ED5219F1199A731A98B03EEFFBE8D02F728E9216B2E55BD5FC3
IVIPR_RE90019519_ResponsetoNFOA_PC-RXC/SR.pdf	A7A84AD1893657F041BF8826E2DCCF98978DB0F39860442B0AF15F8B5A0464067DF2727FE2D151FC0F5038011DD70B23EDEF2CD004CE6A42C9BA1840CD51224F
IVIPR_RE90019519_DeclarationEx2001_PC.pdf	81CC43AA1E3760DF3C635E494661F1FA8AC4D907A164343E8D9CF2B887C527272ED895138C44613AF3CEF63A0FC51C247A990426EED7FD86D0067A7A6DB28509
IVIPR_RE90019519_Ex2006_P	53614431ED5BF4A35E7B755532D49FA701F8F18E7410A360A8

C.pdf	E6BE37408ED74418B31EB2ABE971222CD1214E723B17356CD AC94B83270F173E59E6AD395BA26C
IVIPR_RE90019519_Ex2008_PC.pdf	978048F7F858CE5BCA3464FEF65D535E9B59C5A237911DEE3 EC1A03DB192D8A4AA1D17F67AA111D7835A2897A5EAE9472 D636328D7F3275FB03F212B9A8643DF
IVIPR_RE90019519_Ex2007_PC.pdf	3FAF03364FB833E607D093AF92B31A4DC852F9EB13C47F68A 72617CFEC4D5ACEC38CB142939516881B8C352018569C7C68 39686C65F790E8FC7C886A76CE454E

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 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.

REMARKS

I. Status of Claims

Claims 30 and 34 of U.S. Patent No. 7,9497,85 ('785 Patent) are under reexamination. Claims 1-29, 31-33, and 35-90 are not subject to this reexamination proceeding.

Pursuant to 37 C.F.R. 1.530(e), Patent Owner identifies the status of all patent claims as follows:

Claims 30 and 34: original and under reexamination;

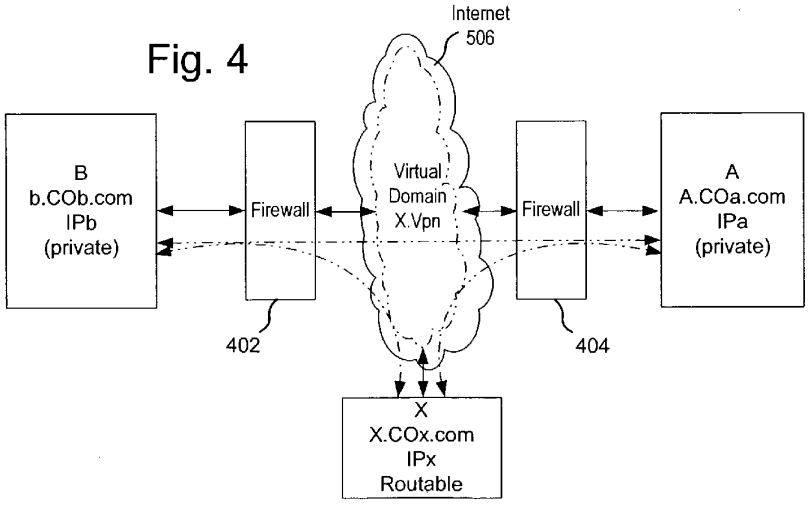
Claims 1-29, 31-33 and 35-90: original and not under reexamination.

II. Example of the Invention

The '785 Patent states that "[a] basic overview of the system is shown in FIG. 4." ('785 Patent, 9:9). Specifically, Figure 4 (reproduced below) shows a Virtual Community Network (VCN) that allows devices, such as A and B, to communicate as if they were on the same physical local network.

AA/SWA Ex. 1015, p.606 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Fig. 4



In an example, the '785 Patent explains that, "[a]s shown in FIG. 4, A, B and X may all make direct connections to each other through communications within the virtual domain. In FIG. 4, dashed lines represent direct communication paths seen to applications running on A, B and X, all "seeing" the virtual addresses of each other and communicating with each other using the application's IP interface." ('785 Patent, 9:36-41). In addition, the '785 Patent explains that "A and B have dynamic or static private IP addresses. Computer or device X is coupled directly to the public Internet and has a public IP address."('785, 9:15-17). The interface between "X.Cox.com IPx Routable" and "Virtual Domain X.Vpn" is an example of a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address. In the example of Figure 4, "X.Vpn" is the domain name defining the virtual network. In this example, the interface for accessing the virtual network from outside the virtual network uses

"X.Cox.com IPx Routable" which has a public network address as identified by the top level domain suffix ".com".

III. Response to Claim Rejections

Issue 1:

- Claims 30 and 34 were rejected under 35 U.S.C. §103 over U.S. Patent No. 7,036,143 to Leung et al. (hereinafter, "Leung") in view of Patent No. 7,155,518 by Forslow (hereinafter, "Forslow") and U.S. Publication No.: 2003/0028671 by Mehta (hereinafter, "Mehta").

Patent Owner respectfully traverses the foregoing obviousness rejections and submits that Claims 30 and 34 recite features not taught, suggested, or otherwise yielded by the primary reference, Leung, or any proper combination of the cited references. Accordingly, the Patent Owner submits that the claims are patentable for at least the following reasons.

A. Mehta, Forslow, And Leung, Alone Or In Combination, Fail To Teach Or Suggest A "Domain Name" As Recited In The Challenged Claims.

Claim 30, recites, in part:

> a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;

None of the cited references teach or suggest "a virtual network that is defined by a domain name having an associated public network address," as recited in Claim 30.

The Office Action relies on Leung for this limitation. However, Leung makes no mention of a "domain name" in any respect, let alone "a domain name having an associated public network address." In order to fill this gap in Leung, the Office Action argues that, "A POSITA would have understood that the subnetwork address obtained from the Internet service provider disclosed in Leung is based on the domain name of the public network" (Non-Final Office Action, Pg. 12). The Office Action cites no evidence in support of this assertion.

It is the Examiner's burden to demonstrate that each and every element of Claim 30 is met by the relied on references, either expressly or inherently. The Office Action does contend that Leung expressly discloses that its subnetwork address obtained from the Internet service provider is "based on the domain name of the public network." That is because Leung makes no mention of a "domain name" -- the term appears nowhere in the reference. Nor does the Office Action allege (let alone demonstrate) that this feature is inherent in Leung. Inherency requires that the limitation *must* be present in the reference, which is not the case here. The fact that the feature is possibly present in the reference is insufficient to demonstrate inherency.

The Patent Owner respectfully submits that obtaining a network address from an Internet service provider (as disclosed in Leung) does not inherently require that such network address is associated with, or based on, a domain name. More specifically, the assignment of an IP address by an ISP does not inherently require a "domain name." For example, in a case where an ISP assigns the network/

subnetwork address of "192.168.1.10" to a customer, there is no requirement the address be associated with, or based on, a domain name -- and ISP's routinely assign network/subnetwork addresses that are not based on, or associated with, a domain name (See Ex. 2001, ¶35).

The Microsoft Computer Dictionary 5th Ed (Ex. 2002) defines a "domain name" as:

> An address of a network connection that identifies the owner of that address in a hierarchical format: server.organization.type. For example, www.whitehouse.gov identifies the Web server at the White House, which is part of the U.S. government (Ex. 2002, Pg. 3).

Similarly, as explained by ""What's In A Domain Name?" A Critical Analysis Of The National And International Impact On Domain Name Cybersquatting" (Ex. 2003):

> For people to find a business web page on the Internet, individuals need to know the business' Internet address. These addresses are extremely important tools for communication. By typing in a certain series of letters, numbers, and symbols, referred to as an Internet domain name, an Internet user gains access to a desired website (Ex. 2003) (internal citations omitted).

Accordingly, a domain name is a human-readable address that identifies a specific location on the Internet, such as a website or an online service. It serves as an *alias* for an IP address, which is the numerical address (e.g., "192.168.1.10") computers use to locate resources on a network. Domain names simplify access to online resources by allowing users to type a recognizable name, like example.com,

instead of a complex numerical IP address. They are structured hierarchically and consist of multiple parts separated by dots, such as www.example.com, where www is the subdomain (optional), example is the second-level domain, and com is the top-level domain (TLD). The Domain Name System (DNS) translates these domain names into their corresponding IP addresses, enabling computers to locate and communicate with the correct servers or devices (see Ex. 2001, ¶32-34). However, there is no requirement that a numerical IP address such as that assigned by the ISP in Leung (e.g., "192.168.1.10") be associated with a domain name maintained by a DNS (Ex. 2001, ¶35).

The Microsoft Computer Dictionary 5th Ed (Ex. 2002) defines an "IP Address" as:

> Short for Internet Protocol address. A 32- bit (4-byte) binary number that uniquely identifies a host (computer) connected to the Internet to other Internet hosts, for the purposes of communication through the transfer of packets. An IP address is expressed in "dotted quad" format, consisting of the decimal values of its 4 bytes, separated with periods; for example, 127.0.0.1. The first 1, 2, or 3 bytes of the IP address identify the network the host is connected to; the remaining bits identify the host itself. The 32 bits of all 4 bytes together can signify almost 232 , or roughly 4 billion, hosts (A few small ranges within that set of numbers are not used) (Ex. 2002, Pg. 4).

Accordingly, a POSITA would understand an IP address to be a unique numerical identifier assigned to each device connected to a network that uses the Internet Protocol for communication. It serves two primary purposes: identifying the host or network interface and providing the location of the device within the network, enabling data to be sent and received (see Ex. 2001, ¶33).

In computer networking, IP addresses are obtained through either dynamic allocation or static assignment, depending on the network configuration. Dynamic allocation, the most common method, is managed by a Dynamic Host Configuration Protocol (DHCP) server. When a device connects to a network, it sends a request to the DHCP server, which assigns an available IP address from a predefined pool. This process is automated and ensures that devices on the network are assigned unique IP addresses without manual intervention. The assigned address is typically leased for a specific duration, after which the lease may be renewed, possibly resulting in a new IP address. This method is widely used in home and enterprise networks due to its simplicity and efficiency (see Ex. 2004).

Alternatively, an IP address can be obtained through static assignment, where a specific address is manually configured on the device. This ensures that the IP address remains consistent and is commonly used for devices that require reliable identification, such as servers, printers, or security cameras. For external-facing devices on the Internet, Internet Service Providers (ISPs) assign public IP addresses, which can be either static or dynamic. Additionally, modern networks may use either IPv4 or IPv6 protocols, with IPv6 designed to address the limitations of IPv4's finite address space (see Ex. 2004).

In neither the static nor the dynamic cases is a domain name required. Instead, when a device connects to a network, the DHCP server assigns it a dynamic IP address according to IETF RFC 2131 (see Ex. 2005). Nowhere does IETF RFC 2131 require that obtaining an IP address require registration with or the existence of a

domain name. In fact, the vast majority of IP addresses (including the laptop utilized to write this document) have been assigned IP addresses and are not associated with a domain name (see Ex. 2001, ¶34).

The same hold true for IP address assigned by ISPs. ISPs assign IP addresses to devices connecting to their networks using methods that depend on the type of connection the user's needs. Most ISPs rely on a DHCP server to assign numerical IP addresses dynamically. When a device connects to the network, it sends a request to the DHCP server, which assigns an available numerical IP address from the ISP's pool along with configuration details like the subnet mask, gateway, and DNS servers. These addresses are leased for a set period, after which the device may either renew the lease or receive a new IP address. In some cases, such as businesses hosting servers or running services requiring remote access, ISPs assign static IP addresses that remain constant. In this case, the ISP manually reserves a numeric IP address for the customer's account and configures it in their network infrastructure (see Ex. 2006). However, in neither case, does the assignment of the numeric IP address by the ISP require an association of the numeric address with a domain name (see Ex. 2001, ¶35).

Therefore, Leung's disclosure that an ISP assigns a public IP address does not inherently teach "a virtual network that **is defined by a domain name** having an associated public network address," as recited in claim 30. As explained by the Federal Circuit, the use of inherency, "a doctrine originally rooted in anticipation, must be carefully circumscribed in the context of obviousness" and "[t]he mere fact

that a certain thing may result from a given set of circumstances is not sufficient to establish inherency" (*Par Pharm., Inc. v. TWi Pharm., Inc.*, 773 F.3d 1186, 1194-95 (Fed. Cir. 2014)) (internal markings and citations omitted). The Court has "emphasized that the limitation at issue necessarily must be present in order to be inherently disclosed by the reference" (*Southwire Co. v. Cerro Wire LLC*, 870 F.3d 1306, 1310-11 (Fed. Cir. 2017)) (internal citation omitted). Therefore, obviousness cannot be established by the mere fact that something may happen inherently. Instead, in the cited reference, the alleged feature must necessarily be present.

Here, as Dr. Noubir explains "that the assignment of IP addresses is completely unrelated to the existence of a domain name. Therefore, there is nothing required in the assignment of an IP address by an ISP to a device that requires the addressee to have a domain name or even be a member of a domain" (Ex. 2001, ¶35).

Further, the '785 Patent makes clear that the assignment of an IP addresses (IPa, IPb and IPx) is completely independent of domain names (X.vpn) (see Fig 4 above). Therefore, Leung does not inherently teach "a virtual network that **is defined by a domain name** having an associated public network address," as recited in the claim 30.

Further, Leung's teaching of a VPN does not inherently require a "domain name." The Microsoft Computer Dictionary 5th Ed (Ex. 2002) defines a "Virtual Private Network" as:

> Nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and

> understood by unauthorized users as if the nodes were connected by private lines (Ex. 2002, Pg. 6).

Accordingly, a POSITA would understand that a Virtual Private Network (VPN) is a secure communication method that creates a connection between a user's device and a remote server over the Internet to replicate the functionality of being connected by a physical wire. The Office Action has proffered no explanation for why computers connected via VPN inherently require a domain name. In fact, the majority of computer networks operate without a domain name. As Dr. Noubir explains, "[t]here is absolutely nothing about a VPN that requires the existence of a domain or the connecting device to have a domain name" (Ex. 2001, ¶36).

Therefore, a POSITA would appreciate that the VPN taught in Leung does not inherently require "a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address."

The suggested additions of Mehta and Forslow do not cure the shortcomings of Leung. The Office Action does not allege, nor do Mehta and Forslow teach a "virtual network that is defined by a domain name having an associated public network address" as recited in claim 30. As a result, Mehta and Forslow, alone or in combination with Leung, fail to teach or suggest every feature recited in claim 30.

Therefore, a *prima facie* case of obviousness has not been established because the combination of the cited references fails to yield the features recited in the claims.

For at least the foregoing reasons, it is respectfully submitted that claim 30 is allowable over Mehta, Forslow, and Leung.

Claim 34 is directly dependent upon claim 30, and the Patent Owner submits the claim is allowable over the cited references of record based on at least its dependency.

Based on at least the arguments presented above, the withdrawal of the 35 U.S.C. §103 rejections of the claims are respectfully requested.

B. Mehta, Forslow And Leung, Alone Or In Combination, Fail To Suggest A DNS Server As Recited In The Challenged Claims.

Claim 30, recites, in part:

> a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.

None of the cited references teach or suggest "a DNS server for the virtual network that is configured to receive a DNS request" and "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device," as recited in claim 30.

Instead, as the Office Action observes, "Leung does not expressly disclose such a DNS server" (Non-Final Office Action, Pg. 26). Accordingly, Leung does not teach a DNS server for the virtual network that is configured to receive a DNS request and "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual

network address associated with the second device," as recited in claim 30. Therefore, Leung fails to teach or suggest every feature recited in claim 30.

The suggested addition of Forslow does not cure the shortcomings of Leung. The Office Action alleges that "A POSITA would have understood that Forslow's mobile service manager 7 functions as a DNS server by receiving HTTPS requests from mobile nodes 3a and/or 3b and returning "user fully qualified domain name 155b/155a, the mobile node 3 private IP address (10.0.0.1) and the virtual home agent's 1a/1b public IP address (204.8.9.1 and 204.8.8.1 respectively)" (Non-Final Office Action, Pg. 26). The Patent Owner submits that Forslow's mobile service manager 7 does not function as a DNS server that "is configured to receive a **DNS request**".

Forslow states that "the mobile nodes 3 a and 3 b … retrieve a list of workgroup members 26 by doing **HTTPS requests** 22 a and 22 b to the mobile service manager 7 and its portal" (Forslow, 10:7-10). However, HTTPS requests are fundamentally different from DNS requests.

The fact that a server receives an HTTPS request and resolves an IP address does make the sever a "DNS server" or the request a "DNS request," as claimed. . A DNS request is responsible for **resolving a domain name**, such as www.example.com, into its corresponding IP address (e.g., 93.184.216.34) to enable devices to locate and communicate with the server hosting the desired resource. Significantly, **a DNS request includes the domain name to be resolved**, and the

response from the DNS server includes a numeric IP address. By contrast, the HTTPS request relied on from Forslow **lacks any domain name**.

The primary protocol used in the Domain Name System (DNS) is the User Datagram Protocol (UDP), which operates on port 53. UDP is a lightweight and efficient protocol that allows DNS queries and responses to be transmitted quickly without establishing a persistent connection. DNS requests are small and efficient, typically consisting of a query for a specific record type (e.g., A, AAAA, CNAME, MX) and a server response containing the requested information. Query latency is further reduced through caching at multiple levels, including local resolvers, ISP-level servers, and content delivery networks (CDNs) (see Ex. 2007)(see Ex. 2001 ¶40).

In contrast, HTTPS requests are designed for secure communication between a client, such as a web browser, and a server, using the HyperText Transfer Protocol over an encrypted SSL/TLS connection. HTTPS operates at the application layer and relies on TCP at the transport layer to ensure reliable data delivery, typically over port 443. The SSL/TLS handshake, which occurs at the start of an HTTPS session, establishes a secure channel by negotiating encryption algorithms, exchanging certificates, and deriving session keys. This process ensures confidentiality by encrypting data, integrity by detecting tampering, and authentication by verifying the server's identity. HTTPS requests involve more complex and voluminous data exchanges compared to DNS, encompassing HTTP headers, cookies, query parameters, and the encrypted payload, which can include sensitive user data or website content. This added complexity increases latency, as the TCP three-way

handshake and the SSL/TLS setup introduce additional overhead (see Ex. 2008))(see Ex. 2001 ¶41).

Accordingly, as explained by Dr. Noubir "a POSITA would appreciate that HTTPS requests and DNS requests are completely different things. For example, the different types of requests operate on different ports, require/ don't require a persistent connection, and perform completely different functions" (Ex. 2001, ¶42). Therefore, Forslow's disclosure of a server that handles HTTPS requests is irrelevant to "a DNS server for the virtual network that is configured to receive a DNS request" and "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device," as recited in the claim 30.

In fact, Forslow is wholly silent with regard to any mention of DNS. Instead, Forslow explains that "The virtual home agents 1 a and 1 b are using the lightweight directory access protocol (LDAP) 25 to retrieve the extranet workgroup configurations" (Forslow, Col. 10:57-60).

The Microsoft Computer Dictionary 5th Ed (Ex. 2002) defines a "Lightweight Directory Access Protocol" as:

> A network protocol designed to work on TCP/IP stacks to extract information from a hierarchical directory such as X.500. This gives users a single tool to comb through data to find a particular piece of information, such as a user name, an e-mail address, a security certificate, or other contact information (Ex. 2002, Pg. 5).

Accordingly, LDAP is a protocol for accessing and managing directory information services over a network. It enables applications to query, search, and

modify hierarchical directories that store data about users, groups, devices, or other organizational resources. Operating over TCP/IP, typically on port 389 for standard communication or port 636 for secure (SSL/TLS) communication, LDAP supports operations such as authentication, searching, and modifying entries. It is commonly used for user authentication, centralized access control, and resource management, integrating with systems like Microsoft Active Directory and OpenLDAP.

Therefore, as explained by Dr. Dr. Noubir "A POSITA would recognize that LDAP and DNS serve fundamentally different purposes and operate with distinct functionalities" (Ex. 2001, ¶44). Specifically, LDAP differs from DNS (in its purpose and functionality, focusing on managing and accessing directory-based information rather than resolving names to network addresses. LDAP is designed for centralized management of user accounts, groups, and permissions, enabling authentication and access control within enterprise environments. Unlike DNS, which primarily maps human-readable domain names to IP addresses for efficient routing, LDAP operates as a protocol for querying and modifying hierarchical directory structures, such as those found in Microsoft Active Directory or OpenLDAP. LDAP relies on TCP for reliable communication, typically over port 389 or port 636 for secure connections, and supports advanced features like secure authentication, role-based access, and integration with Single Sign-On (SSO) systems.

As a result, Forslow's mobile service manager 7 is not "a DNS server for the virtual network that is configured to receive a DNS request" and "return a network address associated with a network route director, a private network address

associated with a second device in the virtual network, and a virtual network address associated with the second device," as recited in claim 30 (Ex. 2001, ¶39). As a result, Forslow, alone or in combination with Leung, fails to teach or suggest every feature recited in claim 30.

Mehta does not cure the shortcomings of Forslow and Leung. The Office Action states, "to the extent it is determined that Forslow's mobile service manager is not a DNS server, it would have been obvious to a POSITA to implement it as a DNS server, as disclosed in Mehta, with the functionality to return the same addresses in the triplet disclosed in Forslow, as well as the public IP address for the route director, as disclosed in Mehta" (Non-Final Office Action, Pg. 31).

The Office Action identifies that Mehta's "FIG. 8 is a process flow diagram showing modifications to the server that can be used to provide a VPN client with the same enterprise address" (Non-Final Office Action, Pg. 23). However, Fig. 8 (reproduced below) shows a routine, implemented by an Address Proxy/Router within an Address Management Proxy System (AMPS), that handles data received from wired devices and facilitates communication with wireless devices by determining the private wireless address corresponding to the invoked public address. It verifies the validity of the address mapping using a TTL parameter, performs any necessary protocol or format conversions, and forwards the data to the wireless device's private address, ensuring compatibility with the wireless network's requirements (See Ex. 2001, ¶46).

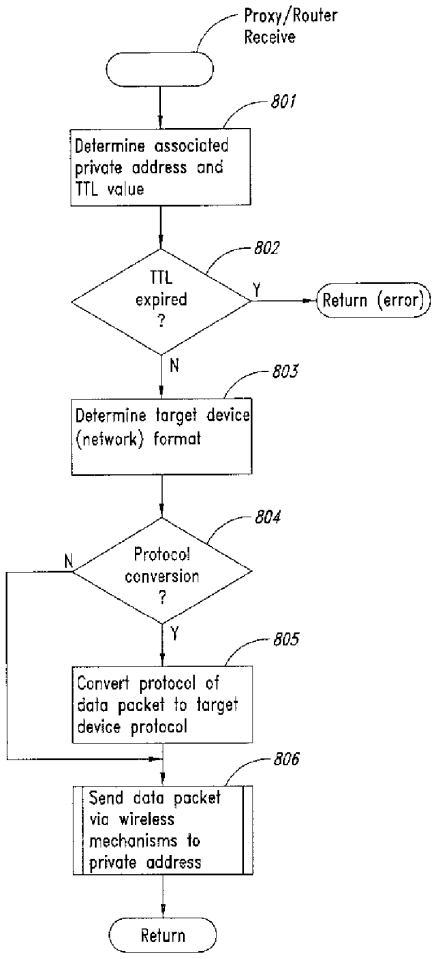


Fig. 8

However, in Mehta the sender only learned the address of the Proxy/Router, and it is the Proxy/Router that does the conversion. The sender is not aware of both the route director and the virtual/private address of the destination. Therefore, Mehta cannot "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device," as recited in the Challenged Claims. Instead, Mehta teaches an architecture that is remarkably

similar to the Dynamic DNS system illustrated in FIG. 3 (reproduced below) of the '785 Patent which is labeled as prior art (See Ex. 2001, ¶47).

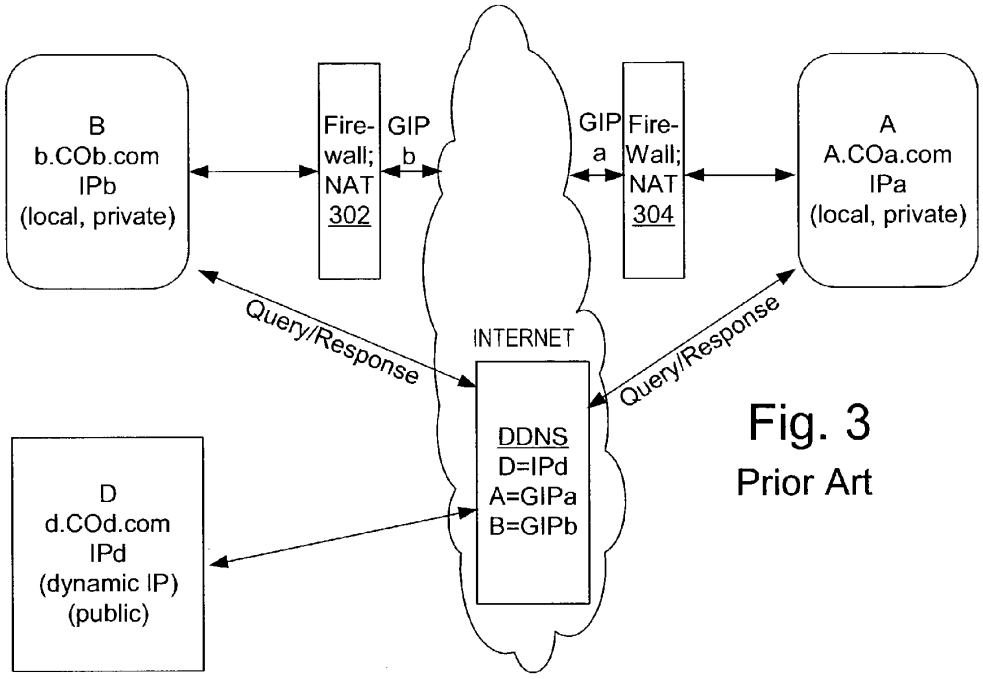


Fig. 3
Prior Art

In fact, providing all three addresses would completely defeat Mehta's purpose of reducing security risks. As explained by the Federal Circuit, "no suggestion to modify a prior art device where the modification would render the device inoperable for its intended purpose" (*Tec Air, Inc. v. Denso Mfg. ch., Inc.,* 192 F.3d 1353, 1360 (Fed. Cir. 1999)). Here, Mehta expressly states, "such addressing capability would expose each device to further security risks, because each such device is part of a publicly accessible network and it becomes more difficult to implement and enforce security measures" (Mehta, ¶025). Therefore, the Office Action's proposed

modification would render the proposed combination inoperable for its intended purpose.

Instead, at most, Mehta allows a client to learn a temporary public IP address from a DNS server. The reference is wholly silent with regard to how to solve the problem of the current invention, which is how to route through a route director to the virtual address. Therefore, Mehta does not teach "a DNS server for the virtual network" that is configured to "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device," as recited in the Challenged Claims.

Instead, the Office Action is impermissibly stitching together an obviousness rejection by not considering Mehta as a whole. Specifically, the Federal Circuit "explains that § 103 does not permit [an Examiner] to stitch together an obviousness finding from discrete portions of prior art references without considering the references as a whole" (*In re Enhanced Sec. Research, LLC*, 739 F.3d 1347, 1355 (Fed. Cir. 2014)). Accordingly, "[i]t is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art" (*In re Wesslau*, 353 F.2d 238 (CCPA 1965)).

Here, Mehta makes it clear that a POSITA would not want to "return a network address associated with a network route director, a private network address

associated with a second device in the virtual network, and a virtual network address associated with the second device," as recited in claim 30 because sharing such information would compromise the security of the internal resources that Mehta is attempting to protect.

Therefore, Mehta, alone or in combination with Forslow and Leung, fails to teach or suggest every feature recited in claim 30. As a result, the Office Action's reliance on Leung, Forslow, and Mehta to reject claim 30 fails to demonstrate that the cited references, individually or in combination, teach or suggest "a DNS server for the virtual network configured to receive a DNS request" and "return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device," as explicitly recited claim 30. Leung lacks disclosure of the DNS server functionality required by the claims, Forslow's HTTPS-based communication does not equate to DNS operations, and Mehta's proposed modifications contradict its stated purpose of maintaining security, rendering the combination inoperable for its intended purpose. Furthermore, the Office Action improperly isolates discrete portions of the references without considering them as a whole, as required under § 103.

Therefore, a *prima facie* case of obviousness has not been established because the combination of the cited references fails to yield the features recited in claim 30.

For at least the foregoing reasons, it is respectfully submitted that claim 30 is allowable over Mehta, Forslow, and Leung.

Claim 34 is directly dependent upon claim 30, and the Patent Owner submits the claim is allowable over the cited references of record based on at least its dependency.

Based on at least the arguments presented above, the withdrawal of the 35 U.S.C. §103 rejections of the claims are respectfully requested.

C. The Office Action Improperly Conflates "Registration" and "Join" Processes, Failing to Establish That the Cited References Teach the Claimed Registration.

Claim 34, recites, in part:

> wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network.

None of the cited references teach or suggest a registration model that is "configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network," as recited in claim 34.

The Office Action states that "A POSITA would have understood that Leung's VPN clients would send registration requests via an associated agent" (Non-Final Office Action Pg. 41). However, the Office Action appears to be conflating a "registration request[1]" with a "join request."

[1] The '785 Patent will expire is several weeks, on or about February 13, 2025. In a reexamination proceeding involving claims of an expired patent, claim construction is controlled by the principles set forth by the court in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). Under *Phillips*, where the specification reveals a special definition given to a claim term by the patentee that differs from the meaning it

The '785 Patent expressly states:

> Registration in this context means registering a machine using a Member Agent or a Group Agent with the VCN Manager. Users may be required to install the Member Agent software. ('785 Patent, 17:10-12)
>
> ***
>
> The registration process is the first step that a user and machine go through with the VCN Manager before becoming a member of a virtual community. There are two phases to member registration: a registration request and a registration file request. Registration happens outside of the IPsec tunnels because at registration time no IPsec tunnel exists for the user registering ('785 Patent, 1740-42).

Accordingly, the '785 Patent defines registration as the process by which the machine and the user are registered with the virtual community. Specifically, the Applicant has acted as their own lexicographer and provided an express definition of registration by stating, "Registration in this context means registering a machine using a Member Agent or a Group Agent with the VCN Manager."

In contrast, the '785 Patent explains the Join/ Leave Process as the following:

> Once a user is registered, the user can join the VCN. Once joined, the user is a member of the VCN. Joining allows the user to let the VCN Manager and other members know that the user/member is on-line and available to communicate. The Join protocol runs between a Member Agent and the VCN Manager to establish a session key with the Manager, authenticate to the Manager, and make use of connections via the Route Directors in the community.

---

would otherwise possess, "the inventor's lexicography governs." Id., at 1316. Thus, to the extent the reexamination proceedings continue beyond February 13, 2025, claim terms such as "registration" must be construed as defined in the specification.

> The Member Join process is illustrated in FIG. 13. There are two phases to the Join operation: phase one is an Initialize Request and phase two is the actual Join. At join time, the IPSec tunnel for secure communication is not established, so the first few join packets are sent outside the IPSec tunnel ('785 Patent, 20:6-18).

Accordingly, the '785 Patent teaches that join/leave process is separate process from the registration process. Specifically, the join/leave process is utilized to establish the connection subsequent to the user and the machine being registered by the registration process.

The Office Action has proffered no evidence that Leung, Forslow, or Mehta, alone or in combination, teach "registering a machine using a Member Agent or a Group Agent with the VCN Manager." Instead, the Office Action cites to Leung's "access request" (Non-Final Office Action, Pg. 39), which is at most analogous to the "join" aspect of the join/leave process in the '785 Patent, as opposed to the registration process which is the subject of claim 34. Accordingly, the Office Action has not established a prima case of obviousness.

To establish a *prima facie* case of obviousness, "there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" (*KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007)). Therefore, the Federal Circuit Court of Appeals requires "record evidence to support an assertion that the structural features of claims ... were known prior art elements" (*K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1365 (Fed. Cir. 2014)). And although "'common sense' can be invoked, even potentially to supply a limitation missing from the prior art, it must still be supported by evidence and a reasoned explanation"

(*Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1363 (Fed. Cir. 2016)). As a result, a *prima facie* case of "[o]bviousness requires a suggestion of all limitations in a claim" (*CFMT, Inc. v. YieldUp Int'l Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003)).

Here, the Office Action has offered no evidence that the cited references teach or suggest a registration model that is "configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network," as recited in the Challenged Claim. As most, the Office Action has suggested that the cited references perform a join function.

Therefore, a *prima facie* case of obviousness has not been established because the combination of the cited references fails to yield the features recited in the claims.

For at least the foregoing reasons, it is respectfully submitted that claim 34 is allowable over Mehta, Forslow, and Leung.

Based on at least the arguments presented above, the withdrawal of the 35 U.S.C. §103 rejections of the claims are respectfully requested

IV. Conclusion

In view of the foregoing, the Patent Owner respectfully request reconsideration. The Patent Owner submits that the U.S. Patent No. 7,949,785, including claims 1-90, is in condition for confirmation of patentability and a solicits a notice to that effect.

Respectfully submitted,

Intellectual Ventures I LLC

By /Brandon R. Theiss/
Brandon R. Theiss
Registration No. 70,507

AA/SWA Ex. 1015, p.630 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R 1.550(f), the undersigned hereby certifies that a copy of Patent Owner's **Patent Owner's Response To Office Action in Ex Parte Reexamination** is being served on January 8, 2025 to Third Party Requester via UPS using Tacking # 1ZR82V53039924673. The copy was sent to:

Unified Patents, LLC
4445 Willard Ave., Suite 600
Chevy Chase, MD 20815

Date: January 8, 2025

By: /Brandon R. Theiss/
Brandon R. Theiss
Registration No. 70,507

AA/SWA Ex. 1015, p.631 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Bibliographic Data

Application No: 90/019,519

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /DENNIS G BONSHOCK/ (Examiner's Signature) | (Initials)

Title: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
05/22/2024	709	3992	IVIPR-RE90019519
RULE			

APPLICANTS

INVENTORS

7949785,

Intellectual Ventures i LLC (Patent Owner), Wilmington, DE, UNITED STATES

Unified Patents LLC (3rd Pty Req.), Chevy Chase, MD, UNITED STATES

Hasan S. Alkhatib, Saratoga, CA, UNITED STATES

Fouad A. Tobagi, Los Altos, CA, UNITED STATES

Farid F. Elwailly, San Jose, CA, UNITED STATES

CONTINUING DATA

This application is a REX of 10403818 03/31/2003 PAT 7949785 *

(*) Data provided by applicant is not consistent with PTO record

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

STATE OR COUNTRY

ADDRESS

VOLPE KOENIG
30 SOUTH 17TH STREET, 18TH FLOOR
PHILADELPHIA, PA 19103
UNITED STATES

FILING FEE RECEIVED

$225

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Examiner	**Art Unit**
	DENNIS G BONSHOCK	3992

CPC								
Symbol							**Type**	**Version**
G06Q	/	10	/	109			F	2013-01-01
G06Q	/	30	/	02			I	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	2	
/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	20 February 2025	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	30	4

U.S. Patent and Trademark Office — Part of Paper No.: 20250219

AA/SWA Ex. 1015, p.633 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	15	/	16

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
709	245

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					
726	15					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	2	
/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	20 February 2025	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	30	4

U.S. Patent and Trademark Office — Part of Paper No.: 20250219

AA/SWA Ex. 1015, p.634 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Examiner	**Art Unit**
	DENNIS G BONSHOCK	3992

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	13	13	25	25	37	37	49	49	61	61	73	73	85	85
2	2	14	14	26	26	38	38	50	50	62	62	74	74	86	86
3	3	15	15	27	27	39	39	51	51	63	63	75	75	87	87
4	4	16	16	28	28	40	40	52	52	64	64	76	76	88	88
5	5	17	17	29	29	41	41	53	53	65	65	77	77	89	89
6	6	18	18	30	30	42	42	54	54	66	66	78	78	90	90
7	7	19	19	31	31	43	43	55	55	67	67	79	79		
8	8	20	20	32	32	44	44	56	56	68	68	80	80		
9	9	21	21	33	33	45	45	57	57	69	69	81	81		
10	10	22	22	34	34	46	46	58	58	70	70	82	82		
11	11	23	23	35	35	47	47	59	59	71	71	83	83		
12	12	24	24	36	36	48	48	60	60	72	72	84	84		

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	2	
/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	20 February 2025	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	30	4

U.S. Patent and Trademark Office — Part of Paper No.: 20250219

AA/SWA Ex. 1015, p.635 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Certificate Date	Certificate Number
		C1

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
Unified Patents, LLC 4445 Willard Ave., Suite 600 Chevy Chase, MD 20815

LITIGATION REVIEW ☑	/DGB/ (examiner initials)	11 June 2024 (date)
Case Name		Director Initials
· 1:24cv344 Assurant, Inc. v. Intellectual Ventures I LLC et al., US District Court, Delaware (OPEN)		
· 2:23cv523, Intellectual Ventures I LLC et al. v. JP Morgan Chase Bank, US District Court, Eastern District Texas (OPEN)		
· 2:23cv524, Intellectual Ventures I LLC et al. v. Comerica Incorporated, US District Court, Eastern District Texas (OPEN)		
· 2:23cv525, Intellectual Ventures I LLC et al. v. Liberty Mutual Holding Company, US District Court, Eastern District Texas (OPEN)		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	**NUMBER**
Inter Partes Review	IPR2025-00201

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.
90/019,519	05/22/2024	7949785	IVIPR-RE90019519	2698

3624 7590 03/06/2025

VOLPE KOENIG
30 SOUTH 17TH STREET, 18TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
03/06/2025	PAPER

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Unified Patents, LLC
4445 Willard Ave., Suite 600
Chevy Chase, MD 20815

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/019,519* .

PATENT UNDER REEXAMINATION *7949785* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Notice of Intent to Issue Ex Parte Reexamination Certificate	**Control No.** 90/019,519	**Patent Under Reexamination** 7949785	
	Examiner DENNIS G BONSHOCK	**Art Unit** 3992	**AIA (First Inventor to File) Status** No

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

1. ☑ Prosecution on the merits is (or remains) closed in this *ex parte* reexamination proceeding. This proceeding is subject to reopening at the initiative of the Office or upon petition. *Cf.* 37 CFR 1.313(a). A Certificate will be issued in view of
   (a) ☑ Patent owner's communication(s) filed: 1/8/2025.
   (b) ☐ Patent owner's failure to file an appropriate timely response to the Office action mailed: _____.
   (c) ☐ Patent owner's failure to timely file an Appeal Brief (37 CFR 41.31).
   (d) ☐ The decision on appeal by the ☐ Board of Patent Appeals and Interferences ☐ Court dated _____
   (e) ☐ Other: _____.
2. The Reexamination Certificate will indicate the following:
   (a) Change in the Specification: ☐ Yes ☑ No
   (b) Change in the Drawing(s): ☐ Yes ☑ No
   (c) Status of the Claim(s):
      (1) Patent claim(s) confirmed: 30 and 34.
      (2) Patent claim(s) amended (including dependent on amended claim(s)): _____
      (3) Patent claim(s) canceled: _____.
      (4) Newly presented claim(s) patentable: _____.
      (5) Newly presented canceled claims: _____.
      (6) Patent claim(s) ☐ previously ☐ currently disclaimed: _____
      (7) Patent claim(s) not subject to reexamination: 1-29,31-33 and 35-90.
3. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
4. ☑ Note the attached statement of reasons for patentability and/or confirmation. Any comments considered necessary by patent owner regarding reasons for patentability and/or confirmation must be submitted promptly to avoid processing delays. Such submission(s) should be labeled: "Comments On Statement of Reasons for Patentability and/or Confirmation."
5. ☐ Note attached NOTICE OF REFERENCES CITED (PTO-892).
6. ☐ Note attached LIST OF REFERENCES CITED (PTO/SB/08 or PTO/SB/08 substitute).
7. ☐ The drawing correction request filed on _____ is: ☐approved ☐disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐None of the certified copies have
   ☐been received.
   ☐not been received.
   ☐been filed in Application No. _____.
   ☐been filed in reexamination Control No. _____.
   ☐been received by the International Bureau in PCT Application No. _____.

   * Certified copies not received: _____.
9. ☐ Note attached Examiner's Amendment.
10. ☐ Note attached Interview Summary (PTO-474).
11. ☐ Other: _____.

All correspondence relating to this reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

/DENNIS G BONSHOCK/ Primary Examiner, Art Unit 3992	

cc: Requester (if third party requester)

AA/SWA Ex. 1015, p.639 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786

Notice of Pre-AIA or AIA Status

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

Notice of Intent to Issue a Reexamination Certificate

This is a Notice of Intent to Issue a Reexamination Certificate in the Ex Parte Reexamination of claims 30 and 34 of United States Patent Number: 7,949,785 issued to Alkhatib et al. (hereinafter the '785 Patent). The Reexamination was ordered on 6/14/2024 responsive to the Request for *ex parte* reexamination filed 5/22/2024, with a Non-Final office action issued on 10/8/2024. This action is responsive to the Response to Office Action dated 1/8/2025.

References

- U.S. Patent No. 7,036,143 to Leung et al. (hereinafter Leung)
- U.S. Patent No. 7,155,518 to Forslöw et al. (hereinafter Forslöw)
- U.S. Publication No. 2003/0028671 to Mehta et al. (hereinafter Mehta)

Prosecution History

Original Examination:

The 7,949,785 patent resulted from the 10/403,818 application which was filed on March 31, 2003.

On 9/22/2006, the Office issued a Non-Final Office action rejecting all claims under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application No. 2003/0041136 to Cheline et al.

On 3/22/2007, Patent Owner (then Applicant) filed a response with a series of amendments to the claims. Specifically, noting that the network traffic router "uses router data to route traffic between members of the virtual community" and that "a first member of the virtual community communicates with another member in the virtual community by querying the DNS server to determine a virtual network address and a private network address for the another member, and to determine a public address of the network traffic router."

On 6/5/2007, a Final Office action issued rejecting all claims either over Cheline alone or Cheline in view of US Patent Publication No. 2004/0006708 to Mukherjee.

On 12/4/2007, Patent Owner filed an RCE heavily amending the claim set

On 2/4/2009, the Office largely rejected most claims under 35 U.S.C. 101 as being directed toward "software elements". Then rejecting the amended claims under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application No.: 2008/0232295 by Kreiner et al. Examiner further noted that *"Claims 16 and 44 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in*

independent form including all of the limitations of the base claim and any intervening claims." See claim 16 below (claims 44 was similarly worded)

> **16. (currently amended)** The system of claim 1 wherein the virtual network manager is further configured to receive a DNS request from the source device, and return a public network address of the route director, a private network address for the destination device, and the second virtual network address that corresponds to the destination device. ~~claim 15 wherein said second device includes at least one private physical address.~~

On 9/1/2010, the Office issued an office action noting allowability of claims 1-15, 17-24, 26-36, 41-43, and 93-109, noting: *"the prior art was not found to teach or suggest returning a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device in response to a DNS request in the context of claims 1, 32, and 93. Specifically, no examples were found in the prior art of record in which both a private address and a virtual address of a destination device would be returned." The office action further rejected claims 53-66 and 68-92 under* 35 U.S.C. 102(e) as being anticipated by U.S. Patent No.: 6,631,416 to Bendinelli.

On 11/5/2010, the Office issued a non-final office action again returning to rejecting claims 1-15, 17-24, 26-36, 41-43, and 80-92 under 35 U.S.C. 101 as being broad enough to be directed toward "software per se".

On 12/2/2010, the Patent Owner filed claim amendments grounding the claims in hardware.

On 1/14/2011, the Office issued a Notice of Allowability giving no further reasons for allowance.

Litigation History

- 1:24cv344 Assurant, Inc. v. Intellectual Ventures I LLC et al., US District Court, Delaware (OPEN)
- 2:23cv523, Intellectual Ventures I LLC et al. v. JP Morgan Chase Bank, US District Court, Eastern District Texas (OPEN)
- 2:23cv524, Intellectual Ventures I LLC et al. v. Comerica Incorporated, US District Court, Eastern District Texas (OPEN)
- 2:23cv525, Intellectual Ventures I LLC et al. v. Liberty Mutual Holding Company, US District Court, Eastern District Texas (OPEN)

Reasons for Confirmation

The following is an Examiner's statement of reasons for patentability and/or confirmation of claims found patentable in this reexamination proceeding.

Typically, the primary source of prior art in an ex parte reexamination will be the patents and printed publications cited in the request for ex parte reexamination. MPEP

§ 2256. The Examiner had previously applied **Leung (U.S. Patent No. 7,036,143) in view of Forslöw (U.S. Patent No. 7,155,518) and Mehta (U.S. Publication No. 2003/0028671)** when rejecting the claims of the Reexamination. Below the Examiner shows where the applied references are deficient in covering the limitations of the independent claims.

Specifically, the claims specify a "**DNS server configured to receive a DNS request from a first device in the virtual network, and return** a network address associated with a network route director**, a private network address associated with a second device in the virtual network and a virtual network address associated with the second device**". The Examiner had previously relied upon Forslöw for covering the majority of this limitation, as proposed in the Request (all except 'return a network address associated with a network route director' where Mehta was applied). Forslöw teaches the use of a HTTPS request being submitted to a mobile service manager 7 and returning a "user fully qualified domain name 155b/155a, the mobile node 3 private IP address (10.0.0.1) and the virtual home agent's 1a/1b public IP address (2004.8.9.1 and 2004.8.8.1 respectively)" (see Non-Final Office Action page 26).

A HTTPS request is however very different from **a DNS request**. A DNS request essentially starts with the provision of a domain name (e.g. google.com / apple.com / ibm.com) to a DNS server which then provides back the IP address (e.g. 192.8.8.1 / 204.8.9.1) corresponding to the domain name. An HTTPS request, however, generally takes place after a DNS request has been made and an IP address is obtained and is

for the actual secure communication setup and transfer of information to that IP address. Notably, Forslöw does not even start the HTTPS request with the provision of a domain name.

Furthermore what is being returned in Forslöw is the private IP address of one node and the public IP address of the virtual home agent. This is not the same as the claimed "**a private network address** associated with a second device in the virtual network and **a virtual network address** associated with the second device".

The Examiner further notes that the remaining references cited in the reexamination (Leung and Mehta) fail to cure the deficiencies in the Forslöw described above.

Any comments considered necessary by PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

Summary:

Claim 30 and 34 are **CONFIRMED**.

Claims 1-29, 31-33, and 35-90 are **NOT SUBJECT TO REEXAMINATION**.

Conclusion

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

All correspondence relating to this ex parte reexamination proceeding should be directed:

Electronically: Registered users may submit via Patent Center at https://patentcenter.uspto.gov/.

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

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Knox Building
501 Dulany Street
Alexandria, VA 22314

For electronic transmissions, 37 CFR 1.8(a)(1)(i)(C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the USPTO patent electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b)

includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication should be directed to Central Reexamination Unit at telephone number (571) 272-7705.

/DENNIS G BONSHOCK/
Primary Examiner, Art Unit 3992

Conferees:
/JOSHUA D CAMPBELL/
Primary Examiner, Art Unit 3992

/ALEXANDER J KOSOWSKI/
Supervisory Patent Examiner, Art Unit 3992

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/019,519	7949785
	Examiner	Art Unit
	DENNIS G BONSHOCK	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Previous Prosecution History	02/20/2025	DGB
Litigation History	02/20/2025	DGB
Patent Data Portal	02/20/2025	DGB
P-TACTS	02/20/2025	DGB
- IPR2025-00201	02/20/2025	DGB

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

AA/SWA Ex. 1015, p.648 of 648
American Airlines, et. al. v. Intellectual Ventures, et.al.
IPR2025-00786