

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Liberty Mutual Insurance Company, Liberty Mutual Technology Group, Inc.,
Liberty Mutual Holding Company Inc., Liberty Mutual Group Inc., Liberty Mutual
Plano LLC, Comparion Insurance Agency, LLC, Ironshore Holdings (U.S.) Inc.,

and

Comerica Incorporated

Petitioners

v.

Intellectual Ventures I LLC

Patent Owner

IPR2025-00201
U.S. Patent No. 7,949,785

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 7,949,785**

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	GROUND FOR STANDING.....	2
III.	IDENTIFICATION OF CHALLENGE	3
IV.	THE 785 PATENT	3
	A. Overview	3
	B. Prosecution History	12
	C. Person of Ordinary Skill in the Art	14
V.	CLAIM CONSTRUCTION	15
	A. All Claims: “virtual network address”	15
	B. Claim 30, 34, 76: “register module”	16
	C. Claims 35-37, 77-78: “join module”	18
	D. Other Claims.....	21
VI.	PRIOR ART.....	21
	A. Mehta.....	21
	B. RFC-1383	23
	C. Motivation to Combine Mehta and RFC-1383	26
VII.	GROUND 1: Claims 1-2, 6-12, 22, 25-26, 28-49, 51-55, 60-63, 65-66, 72-80, 82-86, and 82-90 are obvious in view of Mehta alone or with RFC-1383	34
	A. The Independent Claims.....	34
	1. Preamble: Virtual network system or manager.....	34
	2. “A virtual network defined by a domain name”	36
	3. Registration/distribution of virtual network address to each device which uniquely identifies the device	38
	4. Route director/routing	44
	5. DNS server, request, and responses	46
	6. A memory and a processor generally.....	54
	B. The Dependent Claims	55

1. Dependent Claims 2, 6-12, 22, 25-26, and 28-29	55
2. Dependent Claims 31-37.....	59
3. Claims 49, 52, 54, 61, 63, and 65-66	61
4. Claims 51, 53, 55, 60, 72 and 73.....	64
5. Claims 76-80, 82-90.....	65
6. Claims 87-88: NAT device limitations	66
VIII. DISCRETIONARY DENIAL IS NOT APPROPRIATE	67
A. 35 U.S.C. § 325(d).....	67
B. 35 U.S.C § 314(a).....	68
IX. MANDATORY NOTICES	70
A. Real Party-in-Interest	70
B. Related Matters.....	71
C. Lead and Backup Counsel and Service Information.....	72
X. CONCLUSION.....	72

EXHIBIT LIST

Exhibit	Description
1001	U.S. Patent 7,949, 785 (filed 2003-31-03, granted 2011-24-05) (“785 patent”)
1002	File History for U.S. Patent No. 7,949,785 (Appl. No. 10/403,818) (“785 FH”)
1003	Reserved
1004	Declaration of Dr. Erez Zadok (“Zadok Decl.”)
1005	Curriculum Vitae of Dr. Erez Zadok
1006	U.S. Patent Application Publication No. US2003/0028671 to Mehta et al. (“Mehta”)
1007	Huitema, C., Network Working Group Request for Comment (RFC): 1383, entitled An Experiment in DNS Based IP Routing (“RFC-1383”)
1008	Reserved
1009	Reserved
1010	Reserved
1011	Reserved
1012	Reserved
1013	Microsoft Computer Dictionary, 3rd ed., 1997, excerpts (“Microsoft Computer Dictionary”)
1014	Andrew S. Tanenbaum, <i>Computer Networks</i> , 2nd ed., 1988, excerpts (“Tanenbaum”)
1015	W. Richard Stevens, <i>TCP/IP Illustrated Volume 1, The Protocols</i> , 1994, excerpts (“Stevens”)
1016	William R. Cheswick & Steven M. Bellovin, <i>Firewalls and Internet Security, Repelling the Wily Hacker</i> , 1994, excerpts (“Cheswick”)
1017	Domain Names - Concepts and Facilities, RFC 1034, IETF, 1987, https://www.rfc-editor.org/rfc/pdf/rfc1034.txt.pdf
1018	Domain Names - Implementation and Specification, RFC 1035, IETF, 1987, https://www.rfc-editor.org/rfc/pdf/rfc1035.txt.pdf
1019	IP Encapsulating Security Payload (ESP), RFC 2406, IETF, 1998, https://www.rfc-editor.org/rfc/pdf/rfc2406.txt.pdf
1020	Dynamic Host Configuration Protocol, RFC 2131, IETF, 1997, https://www.rfc-editor.org/rfc/pdf/rfc2131.txt.pdf

Exhibit	Description
1021	Linux DNS Server Administration, Craig Hunt, 2000, excerpts (“Hunt”)
1022	<i>Intellectual Ventures v. Liberty Mutual</i> , No. 23-cv-525 (E.D. Tex.) – Infringement Contentions
1023	<i>Intellectual Ventures v. Comerica</i> , No. 23-cv-524 (E.D. Tex.) – Infringement Contentions

I. INTRODUCTION

Liberty Mutual Insurance Company, Liberty Mutual Technology Group, Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Group Inc., Liberty Mutual Plano LLC, Comparion Insurance Agency, LLC, Ironshore Holdings (U.S.) Inc., (together, “Liberty Mutual”), and Comerica Incorporated (“Comerica”) (collectively, “Petitioners”) petition for *inter partes* review (“IPR”) of claims 1-2, 6-12, 22, 25-26, 28-49, 51-55, 60-63, 65-66, 72-80, 82-90 (the “challenged claims”) of U.S. Patent No. 7,949,785 titled “Secure Virtual Community Network System”) (“the 785 patent,” EX1001).^{1 2}

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, Abstract. The 785 patent describes a virtual network manager or system that “allows local and remote entities [users] to communicate and collaborate from various locations,”— allowing “two or more users to communicate securely via at least one public network, whether the users are both coupled directly to the public

¹ The Office is authorized to charge fees to Deposit Account 50-3725.

² All emphasis in quotations and annotations/highlights in figures herein has been added, unless otherwise noted.

network, both coupled directly to separate private networks or whether one is in a public network and one is in a private network.” EX1001, 5:48-56.

The 785 patent’s claimed “virtual network manager [/system],” including (1) “a network interface ... for data communication,” (2) “a register module,” (3) a “route director,” and (4) a “DNS server,” does not recite a patentable invention. *E.g.*, EX1001, 36:37-56 (claim 30). The claim elements of the 785 patent, their intended functions, and their arrangements were well-established in the prior art before the 785 patent’s priority date. Additionally, the dependent claims merely reflect incidental details also found in the prior art. Therefore, there is at least a reasonable likelihood that at least one claim of the 785 patent is unpatentable.

Petitioners, supported by the declaration of Dr. Erez Zadok who has over 30 years of experience, demonstrate that the challenged claims are unpatentable. Petitioners respectfully request that the Board institute trial on the grounds presented herein and determine that the challenged claims of the 785 patent are unpatentable.

II. GROUNDS FOR STANDING

Petitioners certify the 785 patent is available for IPR, and they are not barred or estopped from requesting IPR of the challenged claims on the ground identified below.

III. IDENTIFICATION OF CHALLENGE

Petitioners request IPR and cancellation of the challenged claims of the 785 patent on the following ground:

Ground	Challenged Claims	Basis for Rejection
1	1-2, 6-12, 22, 25-26, 28-49, 51-55, 60-63, 65-66, 72-80, and 82--90	§ 103: Mehta (US 2003/0028671A1) and RFC-1383

The 785 patent application (Appl. No. 10/403,818) was filed on and only claims priority to March 31, 2003 (i.e., no earlier applications). EX1001 at 1. Every prior art reference in below ground precedes the 785 patent's claimed priority date.

Reference	Prior Art Date	Status
Mehta (EX1006)	Priority 6/8/2001 Filed 6/10/2002 Published 2/6/2003	§ 102(a), (e)
RFC 1383 (EX1007)	Published 12/1992	§ 102(b)

IV. THE 785 PATENT

A. Overview

The 785 patent claims a “virtual network manager [or system]” that includes several components: (1) a computing device or “network interface configured for data communication,” (2) a “register module configured to register devices in a virtual network,” (3) a router or route director, and (4) a “DNS server configured to

receive a DNS request” from a first (source) device and return three addresses to the source, including “[i)] a network address associated with a network route director, [(ii)] a private network address associated with a second [destination] device in the virtual network, and [(iii)] a virtual network address associated with the second [destination] device.” EX1001, 36:37-56 (claim 30).

Representative claim 30 is below:

[30.0] A virtual network manager, comprising:

[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;

[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:

[30.3] receive a registration request from an agent associated with a device;

[30.4] 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

[30.5] 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.³

The 785 patent identifies the so-called IP address depletion problem as a challenge it was trying to solve to “enable the rapid creation of secure means that allows local and remote specified entities [computer devices] to communicate and collaborate from any location via a standard Internet connection.” EX1001, 1:32-37. The 785 patent indicates that, due to its own popularity, the Internet is “running out of [IP] addresses” that can be assigned to each device, thereby limiting the ability for devices in private networks, for example, to communicate or be accessible via the Internet. EX1001, 1:50-55. The 785 patent also purports to address the “mobility problem,” involving devices being assigned constantly changing/dynamic IP addresses, which other devices on the Internet wishing to communicate with them might find difficult to track. EX1001, 5:10-45. The 785 patent thus describes “a need for a system that provides for local and remote entities to communicate and collaborate using the Internet, [a system that] can work with existing NAT [(Network Address Translation)] devices and firewalls, and allows for devices to move to different physical networks.” EX1001, 2:45-48.

³ Appendix A contains a listing of all challenged claims of the 785 patent.

In the “Description of the Related Art” section, the 785 patent admits that NAT solutions where well known the art, and used to transparently translated between private and public IP address:

One popular solution to the depleting address problem is [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.

EX1001, 1:56-2:7.

One embodiment discloses a “secure Virtual Community Network or (‘VCN’),” described as “a private dynamic network which acts a private LAN for

computing devices coupled to public networks or private networks.” EX1001, 8:66-9:5.

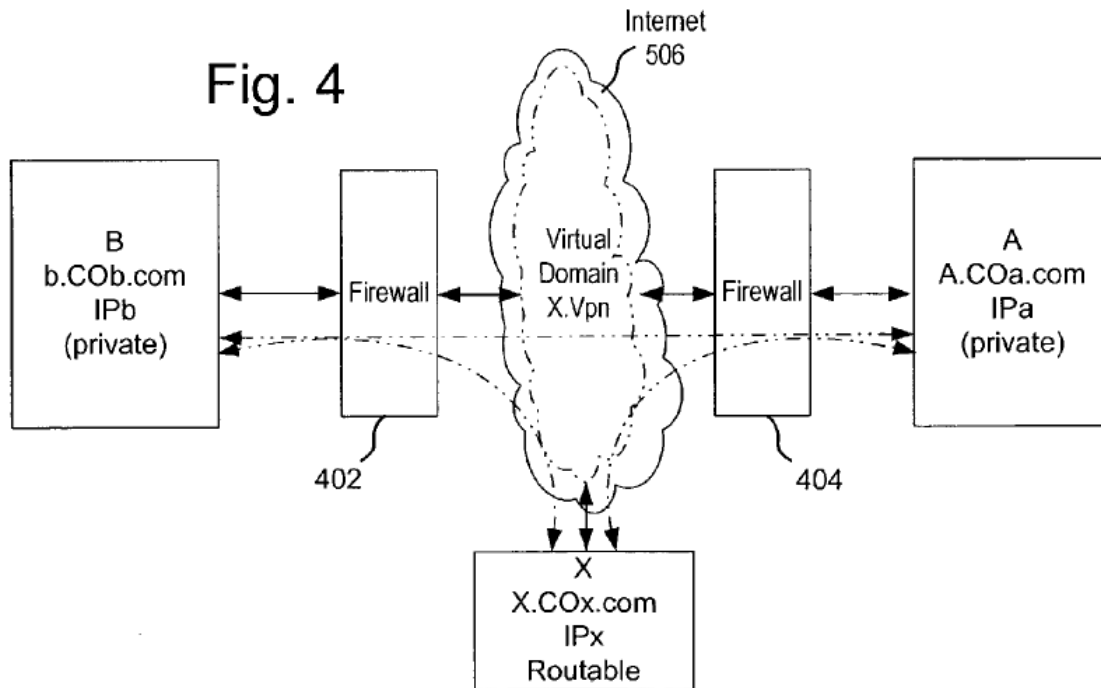
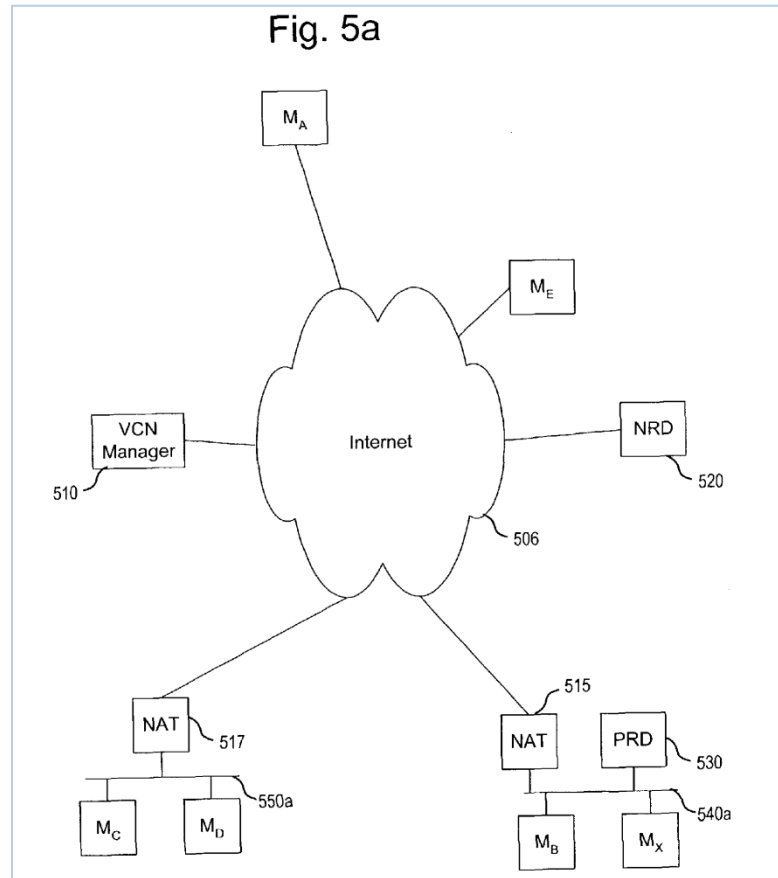


Figure 4 shows an exemplary VCN, which comprises a “computer or device B (host name—b.Cob.com) in a first private domain and computer or device A (host name—a.Coa.com) in a second private domain, both of which are coupled to the Internet by firewall devices 402, 404.” EX1001, 9:9-13. The firewall devices are NAT devices. EX1001, 9:13-15. Moreover, “[c]omputer or device X is coupled directly to the Internet and has a public IP address.” EX1001, 9:16-17. “Devices A, B, and X can join the VCN, leave the VCN, or allows other devices in the VCN to communicate with them.” EX1001, 9:18-23. “All members of the VCN are accessible as if they were part of a physical local network” (e.g. all in the same

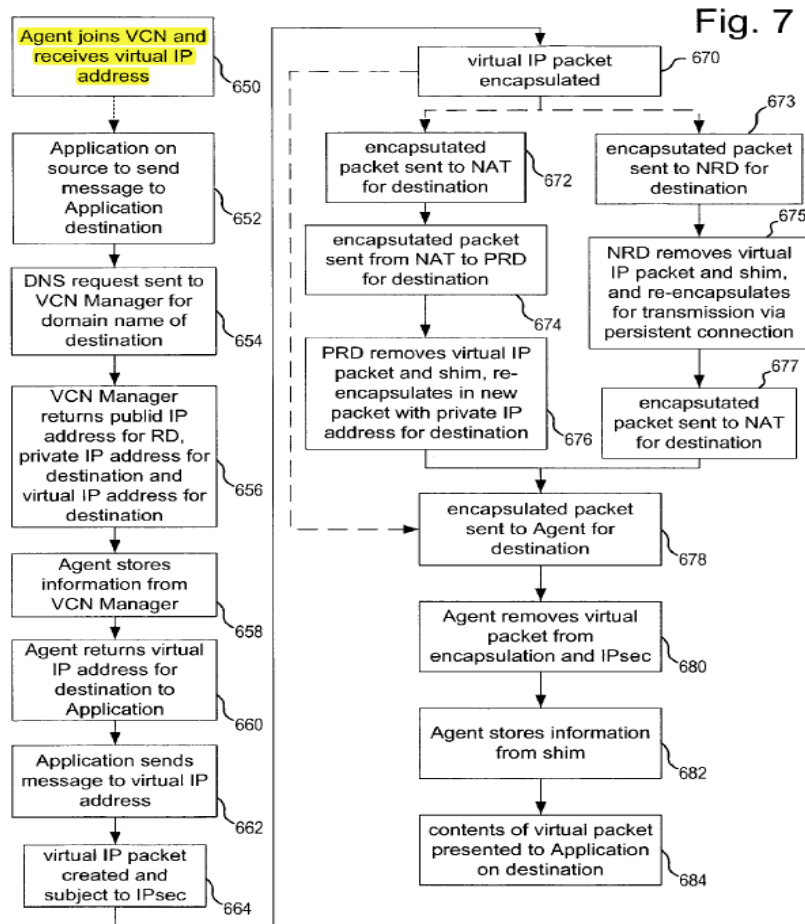
private network)—allowing direct communication between devices within the virtual domain. .EX1001, 9:22-27.

The 785 patent states that “hardware architecture for the machines, servers, or other devices used to implement the present invention should be well understood to one of ordinary skill in the art,” and outlines standard, readily available hardware/software components, including “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.” EX1001, 9:42-48; *see id.* 9:48-54. The patent also states the network interface can include or be connected to a firewall. EX1001, 9:57-60. The network interfaces are inside a computer, and when the computer also functions as a “router,” it “includes two or more network interfaces;” however, “in other embodiments, the computer may include only one network interface.” EX1001, 9:54-56.

Another example of the system is illustrated in Figure 5A. The VCN includes a VCN Manager 510, a Network Route Director 520 and/or Private Route Director 530, and a number of user devices (e.g., M_C , M_X , M_A etc.). .EX 1001, 10:24-27. “The VCN Manager 510 is a central server or server cluster



providing management, connection, and security services for the VCN.” EX 1001, 10:66-11:1. The “various user machines, M_n , are coupled to the Internet 506, as well as other devices.” EX1001,10:17-20. “In order to establish or participate in communication within the VCN, a device must register with and join the VCN, thereby becoming a member.” To join, “[t]he Agent will send a message to the VCN Manager 510 and receive a virtual IP address in return.” EX1001, 14:10-15. This is shown in step 650 of Figure 7. *Id.*



The 785 patent describes the virtual IP or network address as preferably another private network address that is chosen in a well-defined set of addresses (virtual address realm) such that each virtual network address occurs only once across the virtual network and thus is a unique identifier of the device within the network address. EX1001, 12:50-54 (“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 addresses on the Internet.”); EX1001, 12:48-50 (“In general, when choosing virtual addresses it is best to choose addresses

that will not be routable to the member.”). To that end, the 785 patent describes this virtual network address in broad terms, adding that it can be a string, or an address compliant with either IPV4 or IPV6 standards. EX1001, 12:40-44 (“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.”)

As shown in Figure 7, a new member device wanting to send a message to another device in the VCN “will initiate a DNS request,” which is then sent to the VCN Manager 510, as shown in step 654. EX1001, 14:32-34. In response, the “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. EX1001, 14:34-38.⁴ This information is then stored in a table, or any other data structure” for creating a virtual IP packet to be forwarded to the destination address. EX1001, 14:48-15:15. When the destination wishes to respond to the source, or the sources wishes to send additional information, the

⁴ The 785 specification notes that the three addresses are not always returned, for instance, in the case where “the destination machine has a public address (and, thus does not use a routing director) then step 656 will only include returning the public IP address for the destination.” EX1001, 14:40-44.

process of Figure 7 can be repeated, although the steps of performing the DNS request do not need to be performed again, since the information between the two devices has already been stored by the devices. EX1001, 15:58-67.

B. Prosecution History

The application for the 785 patent was filed on March 31, 2003 with a total of 109 claims. During prosecution, the examiner rejected the pending claims numerous times on § 101, 102 and 103 grounds, including based on a number of prior art references. EX1002, 143 (non-final rejection); 203 (final office action); 392 (non-final rejection); 614 (final office action); 687 (rejection).

Of particular relevance to allowance, in an office action dated November 22, 2006, the examiner rejected all claims as anticipated by U.S. Patent Publication No. 2003/0041136 (Cheline). EX1002, 143-162. In response, applicants amended the claims by adding specifically 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 other member, and to determine a public address of the network traffic router.” EX1002, 172-187.

Applicants argued “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), or 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.” EX1002, 190-191.

On September 1, 2010, the examiner issued another office action, stating that then-pending claims 1-15, 17-24, 26-36, 41-43, and 93-109 were allowed, while then-pending claims 53-66 and 68-92 were rejected as anticipated by U.S. Patent No. 6,631,416 (Bendinelli). EX1002, 613-618. The examiner’s reasons for allowance stated 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 that “[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.” EX1002, 616-617.

Applicants subsequently filed an amendment on October 21, 2010, revising some of the rejected claims (claims 53-55, 64, and 80) to include a similar DNS request and corresponding response with a triplet of addresses. EX1002, 658-683.

Following another rejection by the examiner, this time rejecting claims 1-15, 17-24, 26-36, 41-43, and 80-92 as invalid under § 101 while finding that the remaining claims contained allowable subject matter, applicants filed another amendment clarifying that the recited virtual network manager and/or route director are implemented using a memory and a processor of a computing device to traverse the § 101 rejection. EX1002, 687-691. In response, applicants filed an amendment on December 2, 2010, to specify the recited virtual network manager and/or route director are implemented using a memory and processor of a computing device. EX1002, 723-750. A notice of allowance was then issued on January 14, 2011. EX1002, 760-766.

C. Person of Ordinary Skill in the Art

The 785 Patent relates to virtual networking. EX1001, Abstract. A person of skill in the art (“POSA”) at the time of the claimed invention would have had a bachelor’s degree in computer science, computer engineering, or an equivalent degree. A POSA would also have had approximately two years of experience working in the fields of networking including network virtualization, security, and management. Additional experience might substitute for less education and vice versa. EX1004, ¶ 34.

Petitioners' independent expert, Dr. Zadok, qualified as POSA as of the earliest priority date, and remains qualified to testify regarding the understanding of a POSA at the time of the claimed invention. EX1004, ¶ 35.

V. CLAIM CONSTRUCTION

Claim terms are construed according to the *Phillips* standard in an IPR. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. § 42.100. However, claim construction is only required where necessary to resolve a dispute. *See, e.g., Toyota Motor Corp. v. Cellport Sys., Inc.*, IPR2015-00633, Paper 11 at 16 (Aug. 14, 2015) (citing *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011)). Petitioners propose the following claim constructions.

A. All Claims: “virtual network address”

All of the claims of the 785 patent recite a “virtual network address” that is assigned to a device once it is registered in the virtual network. The 785 patent explains a “virtual network address” is a name or address that can be used to identify and send communications to other devices in the virtual network. *See* EX1001, 6:1-7, 31:24-43.

B. Claim 30, 34, 76: “register module”

Claims 30, 34, 76 recite a “register module”⁵ for performing certain functions.

“Module” is a nonce word that substitutes for “means” for purposes of § 112, ¶6.

See Williamson v. Citrix Online, LLC, 792 F.3d 1339, 1350 (Fed. Cir. 2015) (en banc).

[30.2-30.4] 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	Nonce word for “means” function without recitation of structure to perform it
[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.	

⁵ In the litigation, Patent Owner asserts claim 30 and 34 and reads the “registration module” very broadly against commonly and widely used open-source software known as Kubernetes. *See* EX1022 and EX1023 at Claims 30 and 34. Patent Owner contends this term is not a means-plus-function limitation.

Means-plus-function claims are construed by identifying the claimed function and the corresponding structure in the specification for performing it. See *Williamson*, 792 F.3d at 1351. The chart below provides these constructions.

<u>Claims</u>	<u>Function</u>	<u>Structure in 785 Specification</u>
30	“receiving registration request from device’s agent and distributing a virtual network address to the device when it registers with the virtual network.”	“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 Diffie-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 Diffie-Hellman value in octets, and the members initial Diffie-Hellman value.” EX1001, 18:18-29.
34	“receiving registration request from the agent installed on device for data communication via the virtual network.”	<i>Id.</i>

C. Claims 35-37, 77-78: “join module”

Claims 35-37, 77, and 78 recite a “join module”⁶ performing the below described functions. *See Williamson*, 792 F.3d at 1350 (“Module” is a nonce word that substitutes for “means” for purposes of § 112, ¶6.). Claim set 25-37, discussed below, is illustrative.

[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.	Nonce word for “means” function without recitation of structure to perform it
[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.	
[77] The system of claim 75 wherein the virtual network manager includes a member join module.	

⁶ See EX1022 and EX1023 at Claims 35-37 for Patent Owner’s broad constructions.

[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.	
--	--

Means-plus-function claims are construed by identifying the claimed function and the corresponding structure in the specification for performing it. See *Williamson*, 792 F.3d at 1351. The chart below provides these constructions.

<u>Claims</u>	<u>Function</u>	<u>Structure in 785 Specification</u>
35	“receiving join and leave requests from the device or its agent indicating that the device is connected or will be disconnected from data communication, respectively”	The Member Join process is illustrated in FIG. 13 and the leave process in FIG. 14. Fig. 13 <pre> sequenceDiagram participant VM as VCN Manager 510 participant MA as Member Agent 565 Note over MA: Member Attempts to Authenticate 1302 MA->>VM: Init Request 1304 Note over VM: 1306 If packet abnormal, Drop 1308 If member fails authentication, send Init Nack VM->>MA: Init Ack 1314 Note over MA: Member attempts to Join 1316 MA->>VM: Join Request (or Radius Join) 1318 Note over VM: 1320 If packet abnormal, Drop 1322 If Join fails, then send Join Nack VM->>MA: Join Ack 1328 Note over MA: Member now Joined 1330 </pre>

		Fig. 14 <pre> sequenceDiagram participant VCN_Manager as 510 VCN Manager participant Member_Agent as 565 Member Agent Note over VCN_Manager: 1414 If packet abnormal, Drop Note over VCN_Manager: 1416 If member fails authentication or is not Joined, Send Leave Nack Note over VCN_Manager: 1420 If member passes authentication, was Joined and successfully left, Send Leave Ack Member_Agent->>VCN_Manager: 1412 Leave Request VCN_Manager-->>Member_Agent: 1418 Leave Nack VCN_Manager-->>Member_Agent: 1430 Leave Ack Note over Member_Agent: 1410 Member attempts to Leave Note over Member_Agent: 1440 Member successfully Leaves </pre> See also EX1001, 20-21 (for description of figures).
36, 78	“providing virtual network addresses to the devices that are registered in the virtual network”	<i>Id.</i>
37	“maintaining data to associate a virtual network address with a device in the virtual network.”	<i>Id.</i>
77	N/A	

D. Other Claims

No express construction of the other challenged claims is necessary in this IPR because the prior art renders these claims obvious under any reasonable construction.⁷

VI. PRIOR ART

A. Mehta

Mehta, entitled “Method and System for Two-way Initiated Data Communication with Wireless Devices,” describes a system designed to enable secure, bi-directional communication between public network devices and wireless devices on private networks. EX1006, Abstract. Mehta discloses an Address Management Proxy System (AMPS) that allocates temporary public IP addresses to wireless devices to facilitate communication across public and private networks without exposing private IP addresses. EX1006, Abstract. Mehta’s system,

⁷ Petitioners do not concede no construction of the claims may ever be necessary or any other claim construction argument. Should any subsequent discussion of claim interpretation arise here or in the parallel district court proceeding, Petitioners reserve the right to propose constructions and respond to any construction advanced by Patent Owner, the Board, and/or the District Court.

illustrated in Figure 3, includes modified DNS/API servers, Address Proxy/Routers, and an Address Management Data Server to dynamically assign public IP addresses to private network devices as needed. EX1006, [0011].

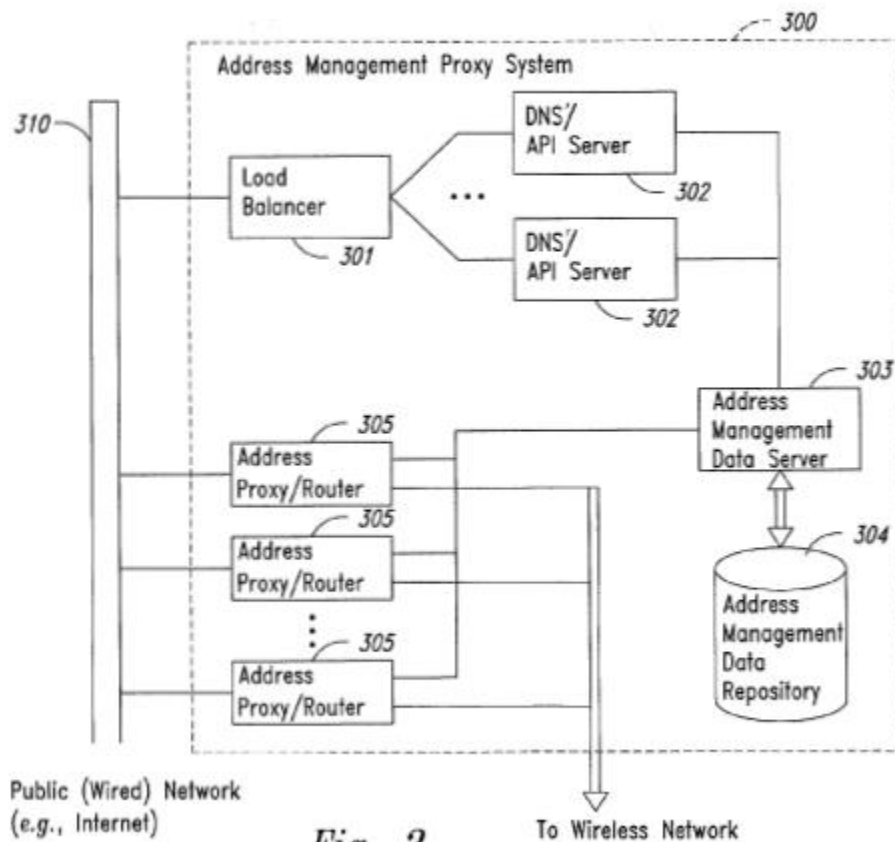


Fig. 3

Metha's AMPS uses techniques like Time to Live (TTL) for each IP mapping, ensuring temporary mappings that enhance security by automatically expiring connections. EX1006, [0015]. The system manages a pool of public addresses to allocate dynamically, using protocols like TCP/IP and UDP for seamless data exchange. EX1006, [0011], [0024]. AMPS can support various types of networks

and devices beyond traditional IP networks, including ATM networks and other wireless technologies. Metha addresses the challenge of secure and efficient communication between disparate network types, enhancing connectivity options without compromising network security. EX1006, [0041].

B. RFC-1383

Request For Comment 1383: An Experiment in DNS-Based IP Routing by Christian Huitema outlines a proposal for utilizing DNS records for IP routing. RFC-1383 seeks to solve the issue of “routing explosion” on the Internet caused by the increasing number of networks, resulting in larger routing tables, more data in route exchanges, and slower responses to routing events. EX1007, 1-2.

RFC-1383 discloses “a scheme that allows for simple routing” that is “complementary with the classic hierarchical routing approach,” while providing “an easy to implement and low cost solution for ‘multi-homed’ domains.” EX1007, 2. Specifically, the RFC-1383 solution is described as “a generalization of the ‘MX record’ scheme used for mail routing.” EX1007, 2,

Similar to the aforementioned mail routing model that uses MX records, RFC-1383 introduces “RX records” for routing IP packets by associating domain names with preferred gateways by means of “source routing” or “tunneling,” or another form of encapsulation protocol. EX1007, 4. To implement this RX routing, a

modified DNS lookup is suggested: the source or an early relay makes the routing decision by querying the DNS for RX records, which list gateways with preference levels. EX1007, 6, 9. This approach avoids hop-by-hop routing updates across the network and is scalable. EX1007, 4.

RFC-1383 describes a network interface integrated with a standard IP router, working alongside a DNS query manager. EX1007, 12-13. When an Internet Control Message Protocol (ICMP) message is received, the query manager updates the local routing table to ensure that any new packets bound for the specified destination are routed through the real-time forwarder. *Id.* Simultaneously, the query manager sends a DNS request to read the RX records for the destination. *Id.* Upon receiving the response, the query manager selects a gateway and provides this information to the real-time forwarder. EX1007, 11-12.

When the real-time forwarder receives a packet, it checks if a gateway for the destination is available. EX1007, 12-13. If so, it inserts the necessary source routing information and forwards the packet—either through the general IP routing program or directly to the network interface linked to the intermediate gateway. EX1007 12. Notably, RFC-1383 discloses (a) a way to store and return multiple IP addresses in response to a single query, and (b) identify an address of the destination in the

domain part of the DNS request and response. RFC-1383 proposes using “TXT” DNS records to store that information:

This [TXT] record is designed for easy general purpose extensions in the DNS, and its content is a text string. Each RX record will contain three fields:

- A record identifier, “RX,” to distinguish it from other experimental uses of the “TXT” record.
- A cost indicator, encoded on up to 3 numerical digits.
- An IP address, encoded as a text string following the ‘dot’ notation.

EX1007, 11. RFC-1383 shows an example record:

domain	type	record	value
-. *.27.32.192.in-addr.arpa	IP	TXT	RX, 10, 10.0.0.7

RFC-1383 explains the table shows: “that [] for all hosts whose IP address starts by the three octets ‘192.32.27’ the IP host ‘10.0.0.7’ can be used as a gateway, and that the preference value is 10.” EX1007, 12. The TXT records described in RFC-1383 are simply a domain field containing a destination address, and a string value comprising comma-delimited fields, including an IP address.

C. Motivation to Combine Mehta and RFC-1383

A POSA would have been motivated to combine Mehta and RFC-1383 for at least the following reasons. As an initial matter, DNS is a foundational Internet technology, so much so that it was one of the very first IETF standards. Work on standardizing domain names began in 1981, with the publication of RFC-799, titled “Internet Name Domains”. See <https://datatracker.ietf.org/doc/html/rfc799>; EX1004, ¶233. Several more RFCs ensued and provided extensive detail on DNS. Even the 785 patent recognized the importance and ubiquity of DNS; indeed, it states “[m]ore information about Dynamic DNS can be found in RFC 2136 incorporated herein by reference.” EX1001, 5:12-14. Without being able to name computer hosts and address them uniquely, the Internet would not even exist. See *id.*

Similarly, Mehta briefly describes DNS. “In a typical TCP/IP (inter)network, machines are organized according to a naming hierarchy. One such hierarchy is [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.)” EX1006, [0009]. A POSA would recognize that DNS has been in use and well known for decades prior to the 785 patent’s 2003 priority date, and POSA would have sought out additional DNS details on known methods in the various RFCs and textbooks written on the subject. See EX1004, ¶235.

Mehta also discloses a modified DNS server that serves as a proxy/router for devices on a private network by maintaining a pool of addresses that are dynamically distributed among active devices. “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.” EX1006, ¶ [0030]

Mehta also discloses a DNS query that returns (a) the device’s unique identifier as the domain part of the DNS query response and (b) a public address associated with the active device. “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.” EX1006, ¶[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.” “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," ... One

skilled in the art will recognize that many other string parameter designations could be used.” EX1006, ¶[0057].

Mehta also describes details of some of the well-known APIs used to programmatically access DNS systems. For example, “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.” EX1006, [0009]. Petitioners’ expert, Dr. Zadok, also describes personally using these programmable APIs and tools many times. *See* EX1004, ¶238.

A POSA would have also known that DNS queries can return multiple types of resource records and multiple entries per query. One example is returning multiple IP addresses for a single name. *See* EX1004, ¶239. As an example, Mehta discloses a modified DNS server that can change what and how much is returned as a result of a DNS query. “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.” EX1006, [0013].

Mehta also discloses being able to query information using alternative APIs, not necessarily the standard DNS ones. “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.” *Id.*

A POSA would have appreciated the power that comes with modifying or extending APIs: new, more versatile functionality can be enabled easily. *See* EX1004, ¶242.

Mehta further discloses returning the information using eXtended Markup Language (XML). “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.” EX1006, [0045]. A POSA would have known that data formatted as XML can be easily processed and parsed, and can be used to return an arbitrary number of items of any type. *See* EX1004, ¶243.

Mehta organizes all the information it needs into three tables, seen in Figure 6 (reproduced below). These tables list at least four pieces of information that can be associated with each host: a Unique ID 601, Private Network Address 602, Public Network Address 631, and Proxy/Router machine 621. See EX1006, [0052]-[0056]. Mehta also discloses auxiliary information such as F/U (flag) 632, TTL 633, and “Other ‘connection’ data” 634. EX1006, [0054].

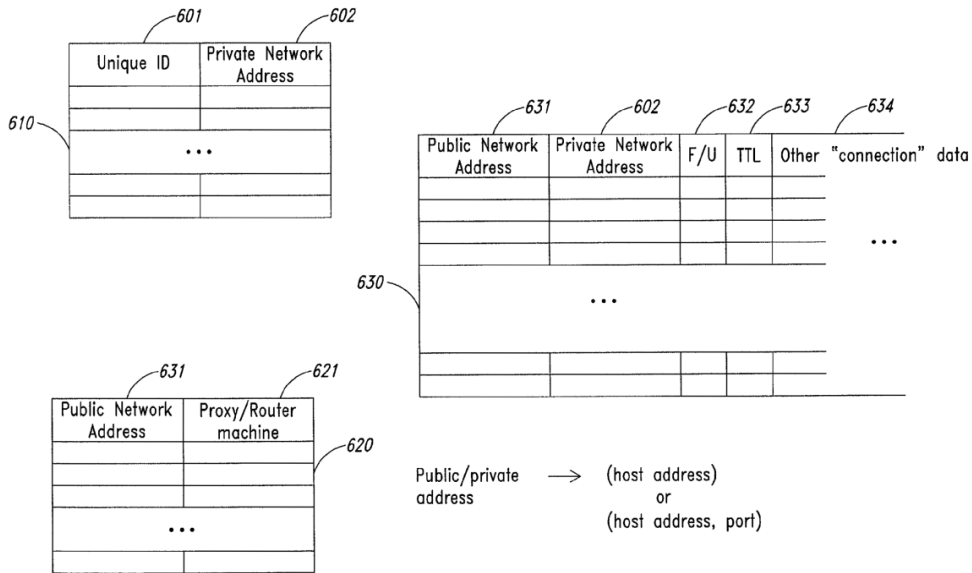


Fig. 6

Taking all these into account, a POSA would have recognized that Mehta (a) discloses a modified DNS server that serves as a proxy/router by maintaining a pool of addresses that are assigned to active devices, (b) discloses a DNS query response that contains a device’s unique identifier and a public address associated with the device, and (c) discloses returning multiple pieces of data and (b) offers

several methods for returning said data. EX1004, ¶246. In other words, Mehta describes a system that routes IP packets based on information stored in DNS. *Id.*

A POSA implementing Mehta's system would have been motivated to seek out additional forms of returning Mehta's DNS information. EX1004, ¶247. Mehta discloses changing the DNS server implementation to enable new functionality. EX1006, [0030]. Changing DNS code requires access to the DNS source code (which is generally opens source) as well as the ability to modify the code, test it, and deploy it. EX1004, ¶247. A POSA would have looked for ways to implement Mehta's solution with less effort, including by utilizing DNS's existing mechanisms. Therefore, a POSA would have found RFC-1383, titled "An Experiment in DNS Based IP Routing." Just from this RFC's title alone, a POSA would have recognized its similarity and applicability to Mehta, because Mehta effectively routes IP packets based on information stored in DNS. EX1004, ¶248.

POSA would have recognized that RFC-1383 goes into more detail about the modified DNS server by disclosing a way to identify an address of the destination in the domain part of the DNS request and response, and to store and return multiple IP addresses in response to a single query, namely "TXT" DNS records having "three fields: [(1)] A record identifier composed of the two characters 'RX' ... used to disambiguate from other experimental uses of the 'TXT' record [(2) a] cost

indicator, encoded on up to 3 numerical digits.... [, and (3) a]n IP address, encoded as a text string following the ‘dot’ notation,” as shown below:

domain	type	record	value
*.27.32.192.in-addr.arpa	IP	TXT	RX, 10, 10.0.0.7

EX1007, 11. The table “means for all hosts whose IP address starts by the three octets ‘192.32.27’ the IP host ‘10.0.0.7’ can be used as a gateway, and that the preference value is 10.” EX1007, 12.

POSA would have appreciated that the TXT records are just a domain field containing a destination address, and a string value comprising comma-delimited fields, including an IP address. EX1004, ¶253. POSA would have found it trivial to use such TXT records to return any number of comma-delimited IP addresses or values, including any of the DNS information disclosed in Mehta. *Id.* Moreover, POSA would have recognized RFC-1383 suggests using TXT records in very similar ways as claimed by the 785 patent: as a resource record with auxiliary information stored in the TXT records. See EX1001, 22:53-57 (“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.”). Parsing data strings in such TXT records using delimiters such as commas is a well-

known technique often taught to first year computer science students. EX1004, ¶255. Indeed, as any user who has used a spreadsheet file knows, a “comma-delimited file” is “[a] data file consisting of fields and records, stored as text, in which the fields are separated from each other by commas. Use of comma-delimited files allows communication between database systems that use different formats. If the data in a field contains a comma, the field is further surrounded with quotation marks.” EX1004, ¶255.

In sum, given how well-known DNS is, a POSA would have found it easy and desirable to modify Mehta with RFC-1383’s TXT record disclosures for routing IP packets using DNS because (a) RFC-1383 provides additional detail about modifications to the DNS server of Mehta that enable multiple addresses to be returned as part of the DNS request and response utilizing standard “TXT” DNS records, and (b) RFC-1383 enhances the unique identifier of Mehta with destination address information by including a destination address in the domain field of the DNS query response. EX1004, ¶256. This obvious change would have been simple and would not have required extensive experimentation or impose undue burden, because DNS is well known, standardized, and widely used. EX1004, ¶257. For the same reasons, the combination would have yielded predictable results. EX1004, ¶257. Lastly, a POSA would have had a high expectation of success because RFC-

1383 merely provides details of one form of returning addresses out of several that Mehta describes. *Id.*

VII. GROUND 1: Claims 1-2, 6-12, 22, 25-26, 28-49, 51-55, 60-63, 65-66, 72-80, 82-86, and 82-90 are obvious in view of Mehta alone or with RFC-1383

A. The Independent Claims

The six independent claims of the 785 patent (claims 1, 30, 38, 48, 62 and 75) recite substantially overlapping subject matter. For ease of discussion, Petitioners address the independent claims together.

These claims generally disclose a virtual network system or manager, comprising a virtual network with a public domain name, a registration feature or module to register devices on the network, a route director to route data traffic between the devices on the network and a DNS server to exchange network addresses of the devices on the network upon request. These limitations, as shown further below, would have been obvious to a POSA before the time of filing of the 785 patent, in light of Mehta alone or combined with RFC-1383.

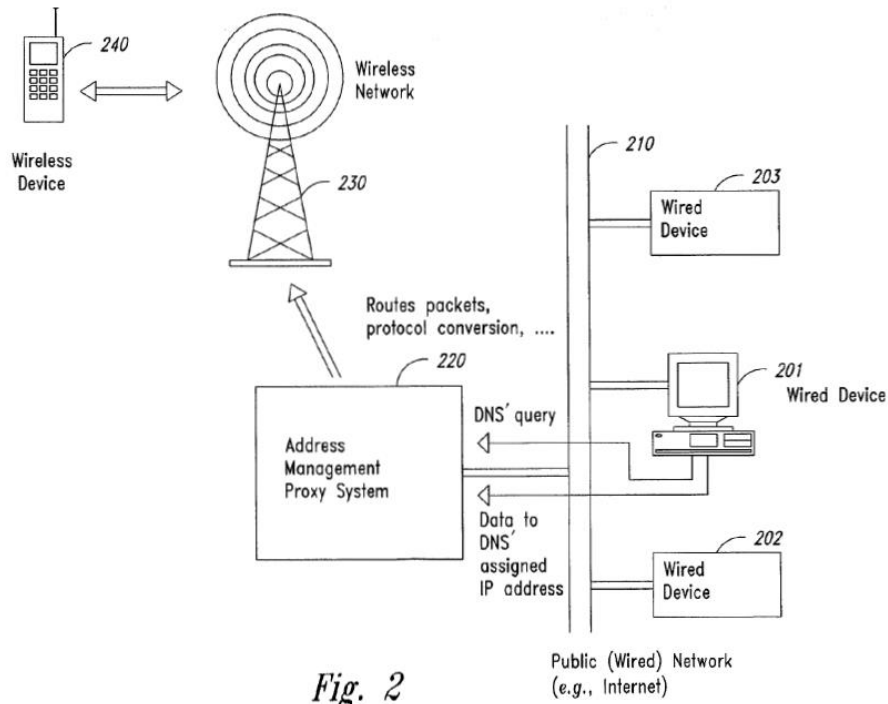
1. Preamble: Virtual network system or manager

Claim	Limitations
[1.0, 1.1]	A virtual network system, comprising a virtual network manager
[30.0]	A virtual network manager, comprising:
[38.0]	A virtual network system, comprising:
[48.0]	A computer-implemented method, comprising:

Claim	Limitations
[62.0, 62.1]	One or more processor readable storage media devices comprising processor readable code that, if executed by a computer device, implements a virtual network manager
[75.0]	A virtual network system , comprising:

To the extent the preambles are limiting,⁸ Mehta discloses an Address Management Proxy System (“AMPS”) illustrated in Figure 2, which is a virtual network system designed to manage communications between “a device on a private network [initiated] from a device on a public network to achieve virtual end-to-end connectivity.” EX1006, [002], claim 67. *See also* EX1004, ¶178-180.

⁸ The 785 patent explains that “[t]he VCN Manager 510 is a central server or server cluster providing management, connection, and security services for the VCN.” EX1001, 10:66-11:1. *See also* EX1004, ¶179.



2. “A virtual network defined by a domain name”

Claim	Limitations
[1.2]	the virtual network manager configured to register devices^[9] in a virtual network that is defined by a domain name
[30.1]	a network interface^[10] configured for data communication via a virtual network that is defined by a domain name having an associated public network address

⁹ POSA would know any system that purports to connect to a computer network includes devices. EX1006, [0033], [0055]; EX1004, ¶181.

¹⁰ Mehta discloses “[e]ach proxy/router machine has a preconfigured set of public network addresses, such as are typically configured by *network cards*

Claim	Limitations
[38.1]	a network manager of a virtual network that is defined by a public domain name
[48.2]	a virtual network that is defined by a domain name having an associated public network address in a public network
[62.2]	a virtual network that is defined by a domain name having an associated public network address in a public network
[75.1]	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

Mehta discloses the AMPS (virtual network system/manager) enables “devices and systems connected to a public internet ... to initiate communication with and to send data to [] devices connected to a private [] network.” EX1006, [0024]. Mehta also discloses the AMPS virtual network community is defined by “public network address[es]” (*see, e.g.*, EX1006, claims 1, 5) that have an associated public domain name, including because Mehta has a DNS or domain name server for the public domain name that returns public IP addresses for associated private devices. *Id.* [0012] (“the AMPS comprises one or more modified DNS’/API servers ... [that] receives a request from a device on a public network for a particular [private network] device, and returns an appropriate temporary public address, which is

[network interface] inserted into the proxy/router machine.” EX1006, [0055], Figs. 1-2; EX1004, ¶181.

internally mapped to the private address of the [private network] device”), [0057] (request for the private network device corresponding to “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.”); *see also* [0048], Fig. 7. *See also* EX1004, ¶181-182.

3. Registration/distribution of virtual network address to each device which uniquely identifies the device

Claim	Limitations
[1.2]	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 network, ¹¹ <i>the virtual network manager further</i>

¹¹ The ’785 patent describes the virtual network address in broad terms, adding that it can be any address compliant with the IPv4 standard, provided that it “will not be routable to the member.” EX1001, 12:40-44 (“These virtual addresses may be any legal IPv4 addresses.”); *Id.* 12:48-50 (“In general, when choosing virtual addresses it is best to choose addresses that will not be routable to the member.”). Any POSA would understand “not directly routable via a public network” to mean not directly routable via a public network **to the member**, because an address that

Claim	Limitations
	configured to distribute a virtual network address to a device when the device is registered in the virtual network;
[30.2-30.4]	[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 ^[12] associated with a device; distribute a virtual network

is routable in the abstract is not necessarily directly routable with respect to a specific device. The temporary public addresses that Mehta discloses are from a pre-assigned pool of public addresses that are dynamically allocated to devices as required, and unusable when not allocated. EX1006, Abstract, (“[A] pool of public addresses, for example, public IP addresses, is maintained by the AMPS and allocated dynamically to [] network devices as required.”); EX1006, [0056] (“...returning the associated public address to the pool of unused public network addresses.”); *Id.* [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.”). Any POSA would understand that unused public network addresses are not directly routable to any destination device.

¹² Mehta discloses a proxy or agent of the device (client programs or specialized API) that communicate with the AMPS on behalf of the device when the

Claim	Limitations
	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;
[38.2-38.3]	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;
[48.1-48.2]	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;
[62.1-62.2]	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;
[75.3]	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,

device needs to register with the virtual network. EX1006, [0025]. *See also* EX1006, [\[0034\]](#).

Mehta discloses that AMPS “dynamically allocates, using methods similar to a DHCP protocol, a private [] network address when the [private network] device registers itself with the [network] infrastructure upon being powered on” that uniquely identifies the device. EX1006, [0053]. “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 [network] infrastructure system.” *Id.*; see also Fig. 3 (showing the Address Management Data Server 303 and Address Management Data Repository 304 where registration information for each device is stored).

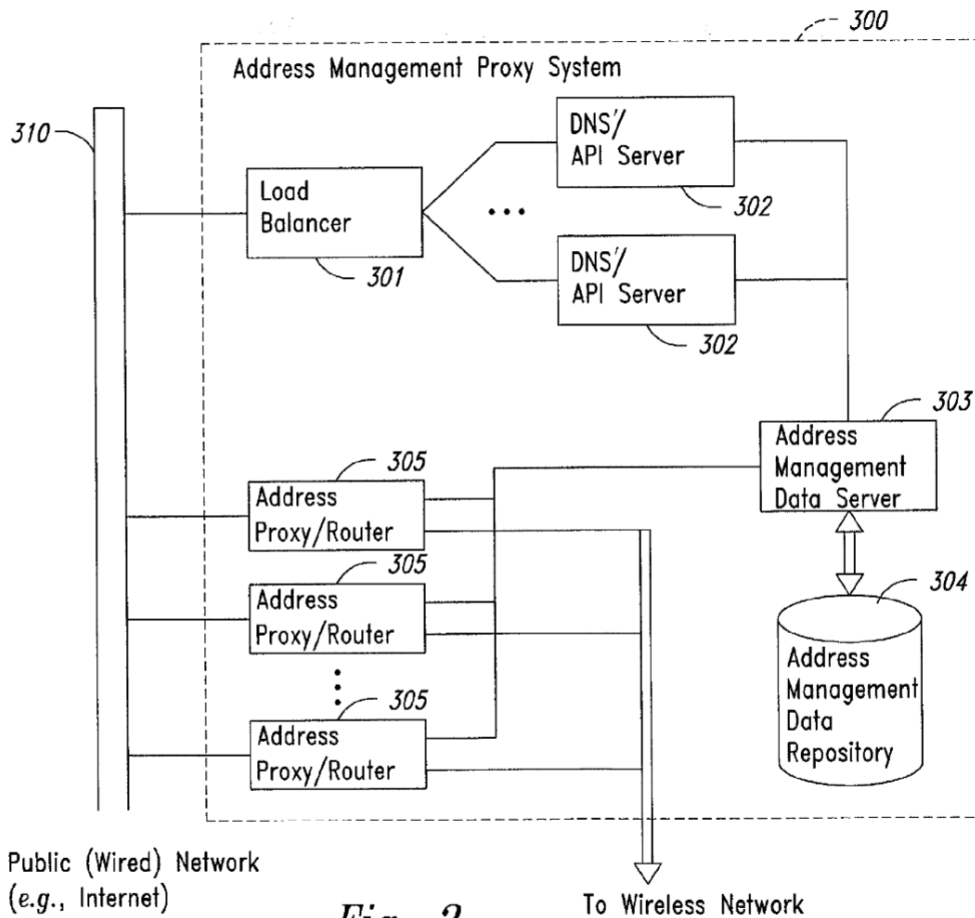


Fig. 3

Mehta also discloses “a pool of public addresses, for example, public IP addresses, is maintained and allocated dynamically to [] network devices as required.” EX1006, [0039]. For example, AMPS “comprises...one or more Address Proxy/Routers” that “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 [virtual network addresses] to [] devices as needed and to update the various mappings between public addresses and the non-routable (private) addresses of the wireless devices.” EX1006, [0032].

Mehta does not disclose the public network address being distributed when the device is registered. However Mehta does disclose that the public network address may already have been assigned at the time the DNS/API server of the AMPS returns a public address in response to a DNS query. “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.” EX1006, [0057]. It would be obvious to a POSA that the public network address could be allocated at the time the device is registered. *See also* EX1004, ¶183-184.

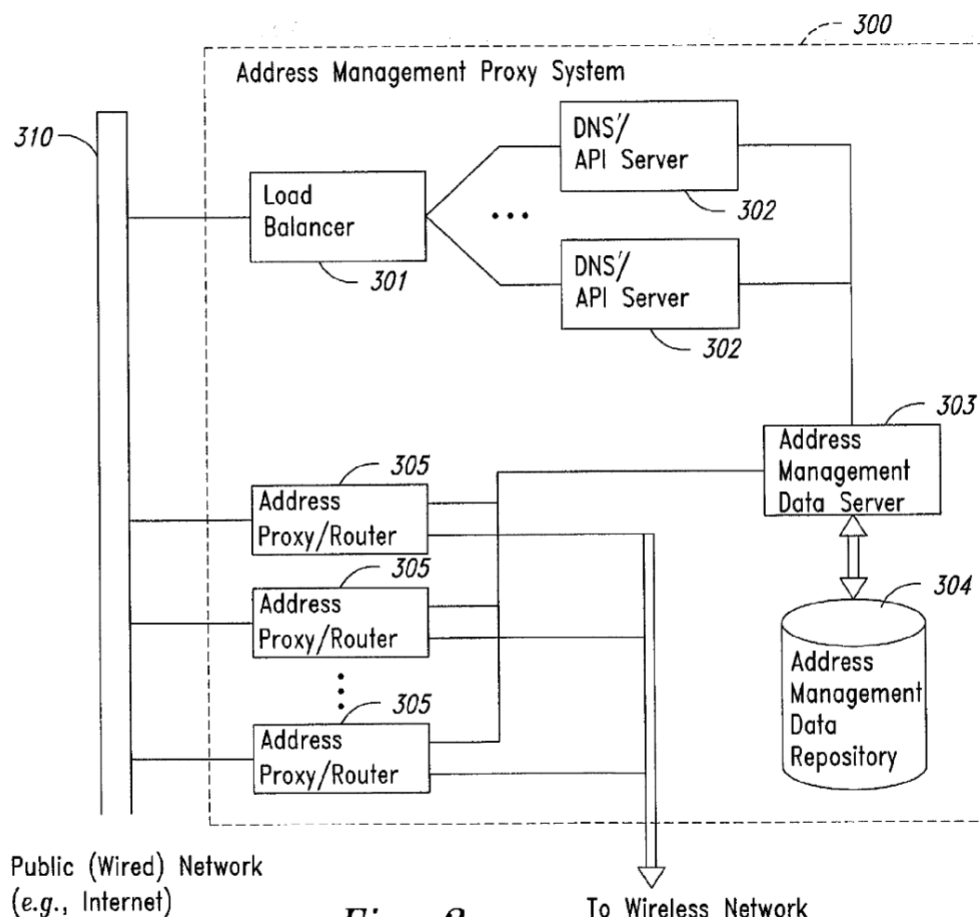


Fig. 3

4. Route director/routing

Claim	Limitations
[1.4]	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 <u>as encapsulated packets</u> 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
[30.5]	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

Claim	Limitations
[38.4]	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 <u>encapsulated packets</u> 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;
[48.4]	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, <u>an encapsulated packet</u> including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device
[62.4]	manage communications routed between the devices that are registered in the virtual network, the communications routed as <u>encapsulated packets</u> 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
[75.4]	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

Mehta discloses a router, or route director (Address/Proxy/Router) for data communications between devices in the virtual network (AMPS). EX.1006, [0012] (“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 router (or routing server/service) contains a routing table, which determines to which machine (and optionally to which port) to send a datagram, given a destination IP address.”

Id. [0008]. “[E]ach [private network] device ends up communicating with the Address Proxy/Router of the other network” to reach other devices on the AMPS virtual network. *Id.* [0033]; *see* [0004], [0010], [0030], [0032], [0036-0038], [0048], [0052], [0055-0059]. *See also* EX1004, ¶185.

Mehta and the knowledge of POSA also disclose the claim elements [38.4], [48.4] and [62.4] that require “encapsulated packets” that include the virtual network addresses of the source and destination devices. Based on Mehta and his own knowledge, POSA would have known that packet encapsulation was well understood and used by 2003. EX1004, ¶186. For example, virtual private networks (VPNs) existed, which utilize packet encapsulation (e.g., embedding one packet inside another). IP Security (IPSec) protocols existed to allow one to transmit secure, encrypted packets, embedded inside plain IP packets. *See* EX1004, ¶187.

5. DNS server, request, and responses

Claim	Limitations
[1.5]	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
[30.5]	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

Claim	Limitations
[38.4]	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
[48.5]	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
[62.5]	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
[75.4]	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

Mehta discloses a DNS server that responds to DNS queries by returning the addresses claimed in the 785 patent, including (1) a public network address of a route director/network manager, (2) a private network address of the destination device, and (3) virtual network address for a destination device. *See* EX1006 [0030] (AMPS “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 Mehta, each (wireless) device has a private IP address and a Unique ID assigned by a (e.g., network) carrier. EX1006, [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.”) Additionally, Mehta has a set of Address Proxy/Router 305 machines, each of which can have multiple public addresses (facing the Internet) as well as multiple private address (facing the wireless network). EX1006, [0055] (“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 When a machine is inserted for use into the AMPS, indications of these addresses are stored [e.g., in field 631].”) *See also* EX1004, ¶188-192.

Mehta organizes this information into three tables, seen in Figure 6 (reproduced below). These tables list at least four pieces of information that can be associated with each host: a Unique ID 601, Private Network Address 602, Public Network Address 631, and Proxy/Router machine 621. Mehta also discloses auxiliary information such as F/U (flag) 632, TTL 633, and “Other ‘connection’ data” 634 that can be in the tables. *Id.* [0052]-[0056]. *See also* EX1004, ¶193-194.

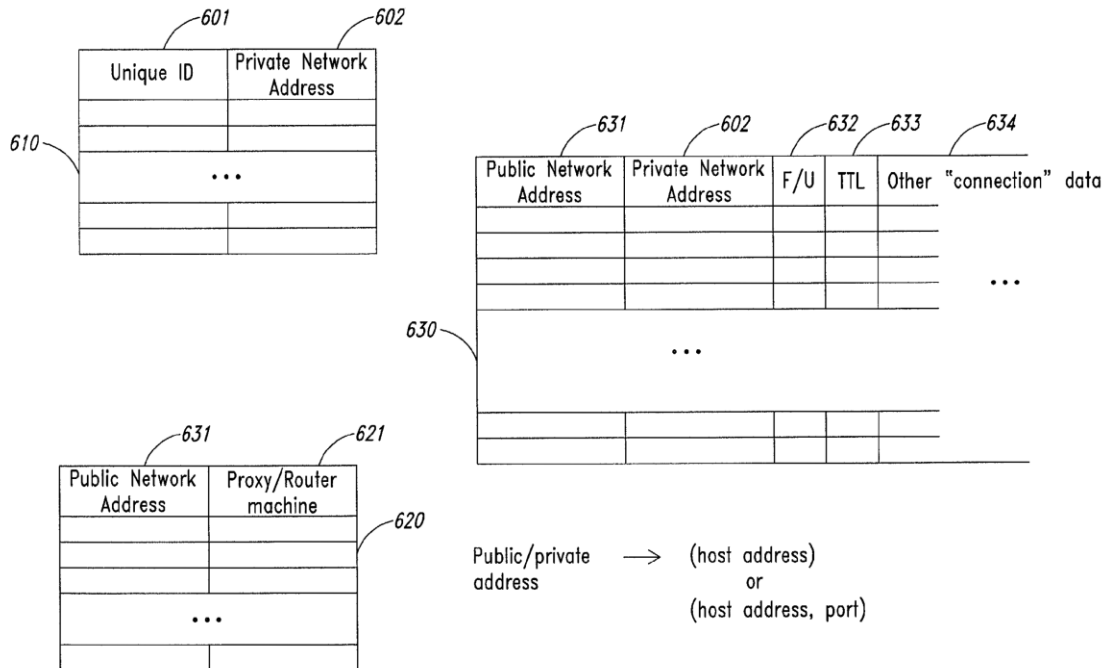


Fig. 6

(1) Public address of route director/virtual network manager: The network route director is Mehta's Address Proxy/Router 305 (any one of them) and Mehta discloses the public address of the Address Proxy/Router [route director] being returned. EX1006, [0057]. ("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 [route director]." EX1006, [0057]. See also EX1004, ¶225-229.

(2) Private network address of destination device:

Mehta discloses that the AMPS stores and assigns to destination devices in the network "a private non-routable address by means of DHCP (or DHCP-like)

server.” EX1006, [0026]. This is the Private Network Address 602 in Tables 610 and 630 of Fig. 6 (shown above). As part of the steps of Fig. 7, the DNS’/API server has to query the Address Management Data Server 303 and it returns this private address from the Data Repository 304. This address is then further returned (upstream) by AMDS 303 to DNS’/API Server 302. This is shown as the red text and arrows in annotated Fig. 3 below. EX1004, ¶217.

Mehta discloses that this private network address (DNS address #2) is returned internally from AMDR 304 to AMDS 303, and to DNS’API Server(s) 302. Mehta, however, does not describe specifically that this private network address is also returned as part of a DNS query. However, a POSA would have been motivated to modify Mehta with RFC-1383 to add this step of returning the private IP address. RFC-1383, returns an “RX” record with private IP address “10.0.0.7.” EX1007, 11.. A POSA would have been motivated to combine the systems and methods in Mehta with the DNS disclosure in RFC-1383 for the reasons discussed in above. *See* EX1004, ¶220-221.

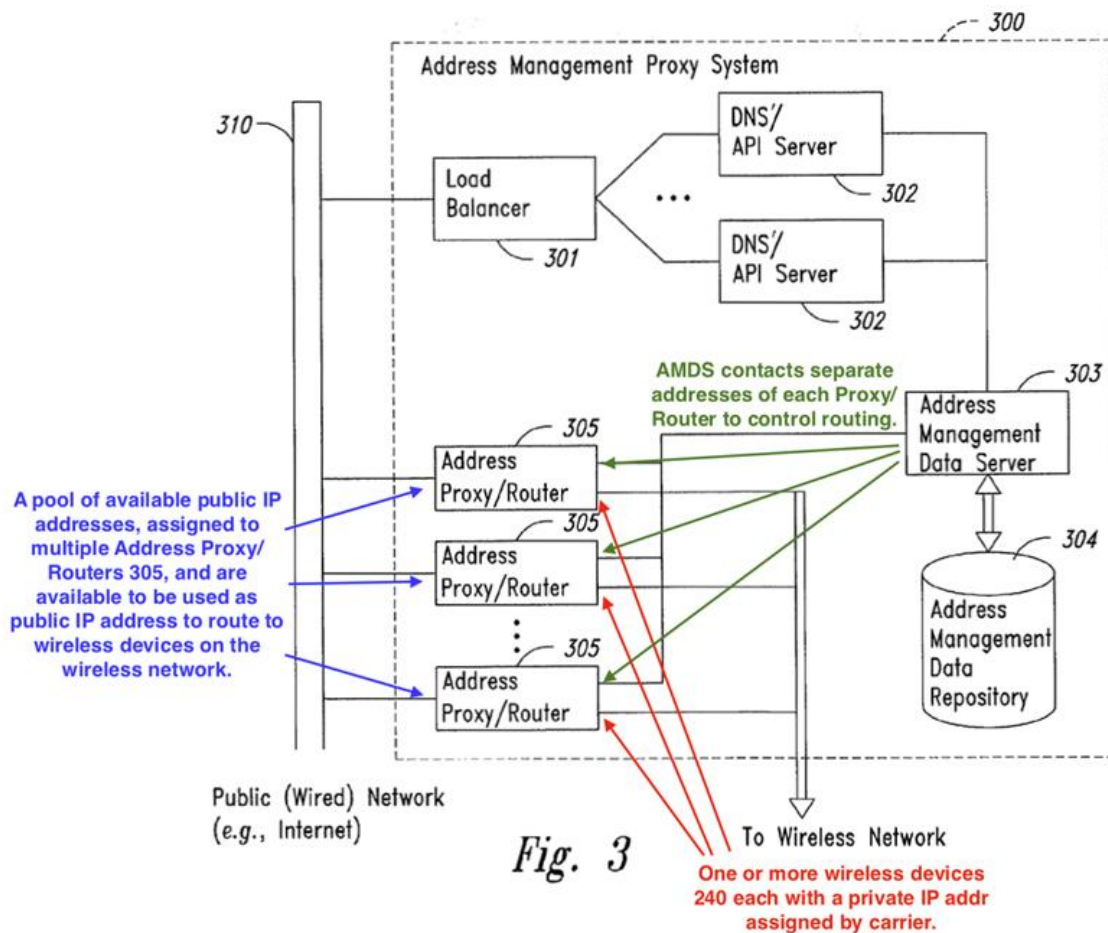
In the alternative, Mehta also discloses a unique identifier that is a unique string name of the device which maps to the private network address assigned to the device. EX1006, [0053]. Mehta also discloses that the unique identifier is used to “[determine] the private [] address of the wireless device designated by a string

parameter passed as input to the [DNS query],” (EX1006, [0057]) and any POSA would recognize that means the unique identifier (DNS address #2) is present in the DNS query and response. EX1004, ¶222.

In another alternative, Mehta also discloses that 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” and that “[o]ne skilled in the art will recognize that many other string parameter designations could be used.” EX1006, [0057]. While Mehta, does not describe that the string parameter includes the private network address, a POSA would have been motivated to modify Mehta with RFC-1383 to add this step of including the private network address (DNS address #2) in the string parameter (“domain” field of RFC-1383), as the private network address maps to the unique identifier for the device, and is itself unique. EX1006, [0052], *see also* EX1004, ¶223.

While Mehta does not disclose encapsulating IP address (e.g., VPN, IPsec). Mehta discloses NAT. EX1006, [0026]. A POSA would have been motivated to improve on Mehta’s NAT techniques by using more modern IP encapsulation and tunneling techniques, such as those disclosed by RFC-1383. Such IP encapsulation explains why a POSA would want the system in Mehta to return a private IP address

in response to a DNS query by combining the system in Mehta with that of RFC-1383. EX1004, ¶224. IP encapsulation, especially IPsec, would have additionally offered transparent packet encryption, an added security bonus. Moreover, by using RFC-1383, the system in Mehta would be improved by using IETF-standardized protocols, improving their interoperability world-wide. EX1004, ¶224.



(3) Virtual network address of destination device: Mehta discloses in “FIG. 7 [] an example flow diagram of an example routine provided by a DNS’/API server of the [AMPS] to return a[n optionally dynamic/temporary] public address that

corresponds to a designated unique identifier... to associate with the [private network device].” EX1006, [0057], [0012]. This corresponds to one of the Address Proxy/Router 621 addresses, out of a pool of many “standby” ones, and is returned in the last step of Fig 7 below. This is also shown as the blue text and arrows in annotated Fig. 3 above. *See also* EX1004, ¶215-216.

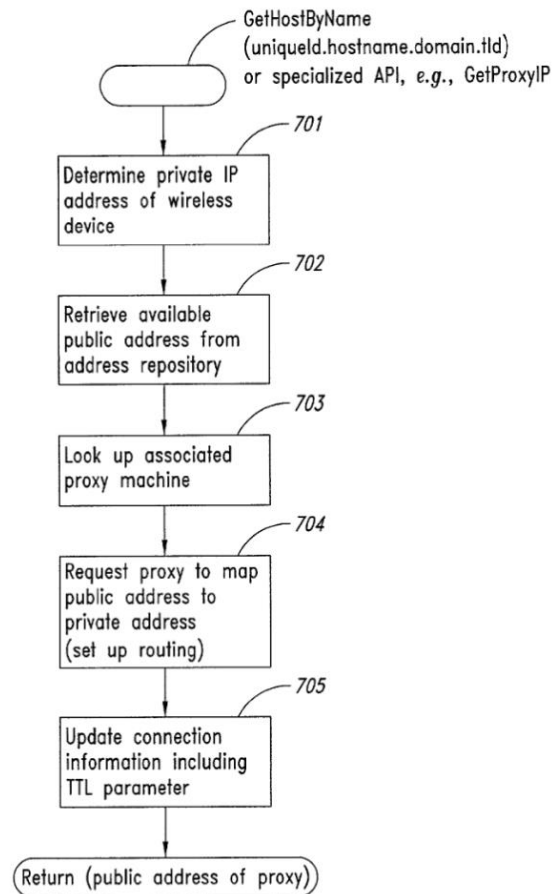


Fig. 7

6. A memory and a processor generally

Some of the independent claims in the 785 patent generically recite memory and processor elements to implement the virtual network manager, route director, or the register/join modules of the virtual network manager. *See* 785 patent [1.1], [1.4], [30.2], [38.1], [62.pre, 62.1], [75.1].

Mehta discloses AMPS and its components are implemented on various computing devices with memories and processors, including Computer System 400, Memory 401, CPU 403, as shown in Figure 4 below. EX1006, [0036], Fig. 4. POSA also would know that Mehta's computerized AMPS system would have memory and processors to implement a virtual network manager, routing director, and register/join modules of the virtual network system. EX1004, ¶230-231.

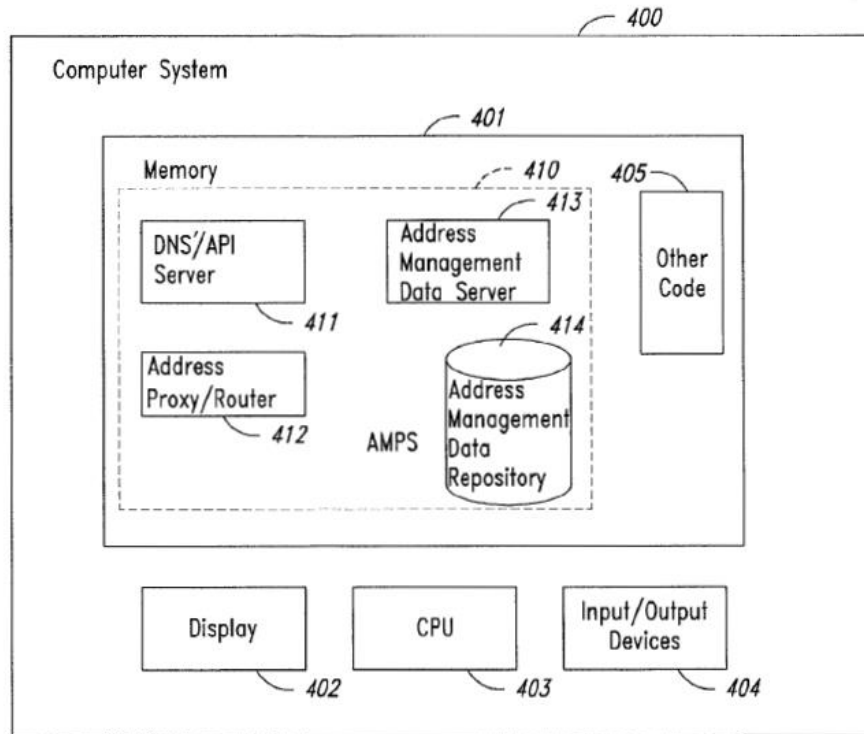


Fig. 4

B. The Dependent Claims

1. Dependent Claims 2, 6-12, 22, 25-26, and 28-29

Claims 2, 6-12, 22, 25-26, and 28-29 depend from Claim 1 and are obvious in light Mehta and RFC-1383 as shown below.

Claims	Prior Art
[2] The system of claim 1 wherein each of the devices communicate with the virtual network manager and the other devices in the virtual	See [1]. Mehta also discloses “client programs” (associated agent) capable of receiving and handling ... incoming communication packets,” including registration requests. See EX1006, [0025]. Devices or blocks within the AMPS “use standard interprocess communication mechanisms to communicate with each other,” which a POSA would understand to include

Claims	Prior Art
network via an associated agent. [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.	agents, processes, or programs installed on the device for data communication. <i>Id.</i> [0036], [0026], [0053]. <i>See also</i> EX1004, ¶260.
[7]The system of claim 1 wherein the virtual network manager is coupled to the public network and has an associated public network address. [22] The system of claim 1 wherein the virtual network manager is coupled to the public network and includes a public network address.	<i>See</i> [1]. Mehta discloses the AMPS (virtual network manager) enabling “devices and systems connected to a public internet.” EX1006 [0024]. <i>See also id.</i> [0033], [0055]. The AMPS has a “public network address” [see cl. 5] and includes a DNS or domain name server with a domain name for the network and associated public IP address. <i>Id.</i> [0012] (“the AMPS comprises one or more modified DNS/API servers.”). <i>See also</i> EX1004, ¶263.
[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.	<i>See</i> [1] and discussion of “encapsulated packets” limitation in Section VII.A.4. A POSA would have understood that encapsulating packets (e.g., using VPN or IPSec) was well known in the art. <i>See</i> EX1004, ¶264.

Claims	Prior Art
[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.	
[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.	<i>See</i> [1]. A POSA would have understood that devices on a network must have a physical network address to communicate. <i>See</i> EX1004, ¶265.
[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	<i>See</i> [9]. A POSA would have understood IP addresses could be assigned dynamically (<i>e.g.</i>, via DHCP) or statically. <i>See</i> EX1004, ¶266-267.

Claims	Prior Art
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.	See [9]. Mehta also discloses a the virtual network manager [AMPS] “dynamically allocat[ing], using methods similar to a DHCP protocol, a private wireless network address when the wireless device registers itself with the [network] infrastructure upon being powered on.” <i>Id.</i> [0053]. A POSA would have also understood that in any network domain where computers can communicate directly, IP addresses must be unique, else computers would not know where to send or receive packets uniquely. <i>See also</i> EX1004, ¶269.
[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.	See [1] and [7] .
[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	A POSA would have also understood that IP addresses could be assigned dynamically (<i>e.g.</i> , via DHCP) or statically assigned, and that DHCP servers can assign private and/or public addresses. <i>See</i> EX1004, ¶279.

Claims	Prior Art
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.	A POSA “will recognize that various other approaches and combinations are possible.” EX1006, [0039]. <i>See also</i> EX1004, ¶280.

2. Dependent Claims 31-37

Claims 31-37 depend from Claim 30 and generally recite additional limitations regarding network interface and/or the registration of member devices in the virtual network. These claims are obvious in view of Mehta and RFC-1383.

Claims	Prior Art
[31] The virtual network manager of claim 30 further comprising an additional network interface configured for data communication via a public network.	<i>See</i> [30]. Mehta discloses “[POSA] will recognize that these devices [(e.g., in AMPS) could be connected to another private or public network.” EX1006 [0030], Fig. 2 (disclosing multiple proxies/routers (e.g., network interfaces) for data communications). <i>See also</i> EX1004, ¶282-283.
[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	<i>See</i> [30] and [31]. Mehta also discloses “[p]orts are typically used to open virtual channels on a single physical address and potentially extend a single physical address to another approximately 65,000 connections. EX1001 [0043], [0042] (“Ports and their implementation are well known in the art.”) The AMPS “can be connected to another TCP/IP based or UDP/IP-based internet.”) <i>Id.</i> [0008]. And “ports are specificized preferably by the Address Proxy/Router

Claims	Prior Art
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.	[network interface]”. <i>Id.</i> [0043]. <i>See also Id.</i> [006], [009], 0010]-[0012], [0014], cls. 107, 108. <i>See also</i> EX1004, ¶284-285.
[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.	<i>See</i> [30]. Mehta also discloses “client programs” capable of receiving and handling incoming communication packets,” including registration requests. <i>See</i> EX1006 [0025]. It further explains that the devices or blocks within the AMPS (e.g., the Address Management Data Repository [“AMDR”]) “use standard interprocess communication mechanisms to communicate with each other,” which a POSA would understand to include agents, processes, or programs installed on the device for data communication. <i>Id.</i> [0036]; <i>see id.</i> [0026], [0053]. <i>See also</i> EX1004, ¶288-289.
[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	<i>See</i> [30]. Mehta also discloses devices “register[ing] and unregister[ing]” themselves with the AMPS (or the carrier infrastructure subsuming the AMPS), and storing device information in the AMDR, which can be “deleted dynamically as devices register and unregister. <i>Id.</i> [0053]; <i>see id.</i> [0026], [0036]. A POSA would have known that protocols like DHCP support commands/messages to join and leave a network. <i>See also</i> EX1004, ¶290-294.

Claims	Prior Art
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.	<i>See</i> [35]. Further, Mehta’s AMDR (join module and part of AMPS) stores and maintains device information, including addresses in mapping tables. EX1006 [0012] (The mapping of addresses associated with a device “is maintained and updated transparently by the AMPS using routing tables and other mapping data structures.”) <i>See also</i> [0032], [0038], [0057], [0059], Fig. 6. EX1004, ¶295-297.

3. Claims 49, 52, 54, 61, 63, and 65-66

Claims 49, 52, 54, , 61, 63, and 65-66, which depend from claim 48 or 62, are substantially identical, so are discussed together. These claims are obvious in view of Mehta and RFC-1383.

Independent Claim 48 Set	Independent Claim 62 Set	Prior Art
[49] The method of claim 48 further comprising providing the devices in the virtual	[63] One or more processor readable storage media devices as recited in claim 62 further comprising processor readable code that, if executed,	<i>See</i> [48] and [62]. Mehta also discloses “client programs” for “receiving and handling incoming communication packets.” <i>See</i> EX1006 [0025]. AMPS “use standard interprocess

Independent Claim 48 Set	Independent Claim 62 Set	Prior Art
network with a communication agent. ¹³	implements the virtual network manager to provide the devices in the virtual network with a communication agent.	communication mechanisms to communicate with each other,” which a POSA would understand to include agents or programs installed on the device for data communication. EX1006 [0036]; <i>see id.</i> [0026], [0053]. <i>See also</i> EX1004, ¶299-303.
[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.	[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.	Mehta discloses the virtual network that includes one or more devices, and the domain name that defines the virtual network. EX1006 [0030], Fig. 2. <i>See also</i> discussion of “virtual network with a domain name” element in Section VII.A.2. <i>See also</i> EX1004, ¶304.
[54] The method of claim 48 further	[66] One or more processor readable	<i>See</i> [48] and [62]. A POSA would have known that

¹³ The 785 patent specifies the “communication agent” is simply a “virtual network adapter interfacing with the device and applications on the devices to route traffic,” i.e., a virtual network card or interface. Ex. 1001, 7:1-5.

Independent Claim 48 Set	Independent Claim 62 Set	Prior Art
comprising assigning the virtual network address to the device as an IPV4 compliant address.	storage media devices as recited in claim 62 wherein the virtual network address includes a non-routable IPV4 compliant address.	Mehta’s 32-bit IP addresses are IPv4 addresses. <i>See</i> EX1006, [0007], [0057]. <i>See also</i> EX1004, ¶305.
[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.	[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.	<i>See</i> [48] and [62] Mehta also discloses several parameters that can be used to enforce policies. “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.” EX1006 [0052]. For example, “once the TTL value indicates that the mapping has expired, the AMPS can destroy the mapping, and also any connection.” EX1006 [0015]. A POSA would have recognized at least the TTL field is controlling and enforcing a policy. <i>See also</i> EX1004, ¶307-308.

4. Claims 51, 53, 55, 60, 72 and 73

Claims 51, 53, 55, 60, 72 and 73 depend from Claim 48 or 62. These claims are obvious in view of Mehta and RFC-1383.

Claims	Prior Art
[51] The method of claim 48 further comprising authenticating the devices as the members in the virtual network.	<i>See</i> [35], [36], and [37]. A POSA also would recognize that devices from a public network (e.g., the Internet) joining a private virtual community network would need to be authenticated for security purposes. <i>See</i> EX1004, ¶311.
[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.	<i>See</i> [48]. Mehta discloses POSA “will recognize that various other approaches and combinations are possible” with respect to the number, arrangement, and configuration of devices in the virtual network. EX1006 [0039]. <i>See also</i> EX1004, ¶313.
[55] The method of claim 54 wherein the IPV4 compliant address is non-routable.	<i>See</i> [54]. Mehta also discloses the method of claim 54 wherein the IPV4 compliant address is non-routable. EX1006 [0007], [0057]. <i>See also</i> EX1004, ¶314.
[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	<i>See</i> [48] and [35] . EX1004, ¶315.

Claims	Prior Art
responding to the join status request to indicate whether or not the second device is joined to the virtual network for data communication.	
[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.	See [67]. A POSA also would have known that IP Security (IPSec) protocols existed to allow one to transmit secure, encrypted packets, embedded (i.e., encapsulated) inside plain IP packets. See EX1004, ¶316-319.

5. Claims 76-80, 82-90

Claims 76-80, and 82-90 depend from claim 75 and are obvious in view of Mehta and RFC-1383.

Claims	Prior Art	Zadok Decl. EX1004
[76]	See [75] and [34].	¶321
[77]	See [75] and [35].	¶322
[78]	See [36].	¶323
[79]	See [37].	¶324
[80]	See [75.4]	¶325
[83]	See [35]	¶327
[85]	See [75.4]	¶330
[86]	See [75] and [34].	¶331

Claims	Prior Art
[82] The system of claim 75 wherein the virtual network manager includes at least a second virtual community definition.	See [75]. A POSA would have understood that computers and network systems/devices could easily define multiple subnets, multiple domains, and more. This is commonplace when configuring DNS and/or DHCP systems for example. EX. 1004, ¶326.

Claims	Prior Art
[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.	See [75.4] A POSA also would have understood that DNS servers are designed to return authoritative responses, else the internet could not even be trusted. EX. 1004, ¶329.
[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.	See [75]. A POSA also would have known that IP Security (IPSec) protocols existed to allow one to transmit secure, encrypted packets, embedded (i.e., encapsulated) inside plain IP packets. <i>See also</i> EX1004, ¶336.

6. Claims 87-88: NAT device limitations

Claims 87 and 88 (depend Claim 75) require a NAT device and are obvious in view of Mehta.

Claims	Prior Art
[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	See [75]. Mehta discloses using Network Address Translation (NAT) “to send data from a [] device to the public networking world.” EX1006 [0026]

coupled to a first private network and accesses a public network via a NAT device	A POSA also would have understood that a Network Address Translation (NAT) device enables devices on private networks to access public networks. EX. 1004, ¶114.
[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.	See [87]. EX. 1004, ¶ 333.

VIII. DISCRETIONARY DENIAL IS NOT APPROPRIATE

A. 35 U.S.C. § 325(d)

None of the combinations of the prior art references relied on herein under §103 (Mehta and RFC-1383), much less the combination of those teachings as informed by a POSA's knowledge and expert testimony, were considered by the examiner during prosecution, nor relied upon in the *ex parte* reexamination request filed by Unified Patents, LLC (Control No. 90/019,519). *See, e.g., Mylan Pharm. Inc., v. Regeneron Pharm., Inc.*, IPR2022-01226, Paper 22 at 27-29 (PTAB Jan. 11, 2023). Further, this petition relies on reference RFC-1383 which was not cited or relied upon during prosecution or in the *ex parte* reexamination. Neither Mehta nor RFC-1383 was considered during prosecution. While Mehta was cited in the reexamination, it was in combination with different references. Notably, this petition

seeks review of over 60 claims of the patent, while only two claims (30 and 34) are subject to reexamination. This Petition thus largely addresses issues that will not be addressed in the reexamination.

Accordingly, this petition should not be denied under Section 325(d).

B. 35 U.S.C § 314(a)

Fintiv and the Office’s interim guidelines dated June 21, 2022 (“Interim Procedures”) favor institution, which best serves the efficiency and integrity of the patent system. Factor 1 is at worst neutral because no request for a stay pending IPR has been filed yet. *Sand Revolution II LLC v. Continental Intermodal Group - Trucking LLC*, IPR2019-01393, Paper 24, 7 (PTAB June 16, 2020) (informative). Nonetheless, Petitioners are considering requesting a stay, which favors institution.

Factors 2 and 3 also favor institution. The related district court cases against Petitioners, filed on November 15, 2023, are in their early stages. The *Markman* process has not begun, no claim construction order has issued, fact discovery remains open and no merits fact depositions have been taken, and expert discovery has not begun. In October 2024, the trial date was extended to September 22, 2025, but on November 5, 2024, after the trial date was moved back, Patent Owner filed a

Second Amended Complaint against Liberty Mutual,¹⁴ an Amended Complaint against Comerica, and finally served source code infringement contentions. Notably, Patent Owner received a lengthy amount of time to provide source code contentions, *i.e.*, from default of 30 days to 75 with extension, and then an additional about 60 days past the 75-day deadline because of Patent Owner's delay. Without the code contentions, Petitioners did not actually know the full details of Patent Owner's infringement theories. In *Sand Revolution*, the district court had "conducted a *Markman* hearing and entered a related Order." IPR2019-01393, Paper 24 at 10. Despite this fact, the Board found that the third *Fintiv* factor "weighs only marginally, if at all, in favor of exercising discretion to deny institution." *Id.* Here, the parallel proceeding is at a substantially earlier phase. Accordingly, these factors weigh against discretionary denial.

As to factors 4 and 5, certain challenged claims were not asserted in the district court, so this Petition addresses issues that will not be litigated there, and this weighs against discretionary denial. Moreover, while Petitioners and Patent Owner are the

¹⁴ Liberty Mutual also has not answered and has a pending motion to dismiss Patent Owner's entire complaint based on improper venue under 28 U.S.C. § 1400(b) since January 2024.

same parties in the district court, this is “far from an unusual circumstance” in IPR and does not warrant discretionary denial. *Sand Revolution*, IPR2019-01393, Paper 24 (instituting where parties were the same).

The Board only addresses Factor 6 if Factors 1-5 support discretionary denial, which they do not. *CommScope Techs. LLC. v. Dali Wireless, Inc.*, IPR2022-01242, Paper 23 (Feb. 27, 2023) (precedential).

This Petition presents a compelling unpatentability challenge. The cited prior art, none of which was cited by the examiner, rebuts the Patent Owner’s arguments during prosecution that persuaded the examiner to allow the claims. Accordingly, the Board should not deny institution under *Fintiv* and the Interim Procedures.

IX. MANDATORY NOTICES

Pursuant to 37 C.F.R. § 42.8(b), Petitioners state:

A. Real Party-in-Interest

The real parties-in-interest are Liberty Mutual Insurance Company, Liberty Mutual Technology Group, Inc., Liberty Mutual Holding Company Inc., Liberty Mutual Group Inc., Liberty Mutual Plano LLC, Comparion Insurance Agency, LLC, and Ironshore Holdings (U.S.) Inc. (“Liberty Mutual”) and Comerica Incorporated (“Comerica”).

B. Related Matters

Patent Owner Intellectual Ventures I LLC (along with Intellectual Ventures II LLC), has asserted the 785 patent (and three other unrelated patents) in:

- *Intellectual Ventures I LLC et al. v. Liberty Mutual Holding Company Inc., et al.*, No. 23-cv-525 (E.D. Tex. filed November 15, 2023)
- *Intellectual Ventures I LLC et al. v. Comerica Incorporated*, No. 23-cv-524 (E.D. Tex. filed November 15, 2023)
- *Intellectual Ventures I LLC et al. v. JP Morgan Chase Bank, National Association et al.*, No. 23-cv-523 (E.D. Tex. filed November 15, 2023)

These cases were consolidated, with the latter Case No. 23-cv-523 as the lead case.

The 785 patent is also asserted in the following cases:

- *Intellectual Ventures I LLC et al., v. American Airlines, Inc.*, No. 24-cv-980 (E.D. Tex. filed November 2, 2024)
- *Intellectual Ventures I LLC et al., v. Southwest Airlines, Co.*, No. 24-cv-277 (W.D. Tex. filed November 2, 2024).

The 785 patent is also at issue in the following declaratory judgment case:

- *Assurant, Inc. v. Intellectual Ventures I LLC, et al.*, No. 24-cv-344 (D. Del. filed March 15, 2024)

The action against JP Morgan has been dismissed with prejudice. The actions against Petitioners and the other cases remain pending. There has been no ruling on claim construction in any case.

The 785 patent is also the subject of an *ex parte* reexamination request filed by Unified Patents, LLC on May 22, 2024 (Control No. 90/019,519). Reexamination was ordered on June 14, 2024.

Petitioners are not aware of any other civil actions or proceedings filed in connection with the 785 patent.

C. Lead and Backup Counsel and Service Information

Lead Counsel	Back-up Counsel
Joshua D. Curry josh.curry@lewisbrisbois.com LEWIS BRISBOIS BISGAARD SMITH LLP 600 Peachtree St. NE, Suite 4700 Atlanta, GA 30308 Ph: 404.348.8585 Fax: 404.467.8845 Reg No. 65,478	François O. Ecclesiaste francois.ecclesiaste@lewisbrisbois.com LEWIS BRISBOIS BISGAARD SMITH LLP Wells Fargo Center 90 S 7th Street, Suite 2800 Minneapolis, MN 55402 Ph: 612.428.5048 Fax: 612.428.5001 Reg No. 75,836

Petitioners consent to service by email to the counsel above.

X. CONCLUSION

For at least the foregoing reasons, Petitioners request IPR be instituted and claims 1-2, 6-12, 22, 25-26, 28-49, 51-55, 60-63, 65-66, 72-80, and 82-90 of the 785 patent be cancelled.

Respectfully submitted,

/Joshua D. Curry/

Joshua D. Curry – Lead Counsel
Registration No. 65,478
LEWIS BRISBOIS BISGAARD SMITH LLP
600 Peachtree St. NE, Suite 4700
Atlanta, GA 30308
Ph: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com

François O. Ecclesiaste
Registration Reg No. 75,836
LEWIS BRISBOIS BISGAARD SMITH LLP
Wells Fargo Center
90 S 7th Street, Suite 2800
Minneapolis, MN 55402
Ph: 612.428.5048
Fax: 612.428.5001
francois.ecclesiaste@lewisbrisbois.com

*Counsel for Liberty Mutual Insurance
Company, Liberty Mutual Technology
Group, Inc., Liberty Mutual Holding
Company Inc., Liberty Mutual Group Inc.,
Liberty Mutual Plano LLC, Comparion
Insurance Agency, LLC, Ironshore
Holdings (U.S.) Inc.*

-and-

*Counsel for Petitioner Comerica
Incorporated*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e) and 42.105(b) and agreement of the parties, the undersigned certifies that on the date indicated below the foregoing document with any attachments was served by email on counsel for the Patent Owner as indicated below.

Brandon R. Theiss
Volpe Koenig
30 South 17th Street, 18th Floor
Philadelphia, PA 19103
btheiss@vklaw.com

Jonathan K. Waldrop
Kasowitz Benson Torres LLP
333 Twin Dolphin Drive, Suite 200
Redwood Shores, CA 94065
jwaldrop@kasowitz.com
IntellectualVentures@kasowitz.com

Date: 11/20/2024

/Joshua D. Curry/

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioners certify that the foregoing IPR petition contains 13,249 words, excluding the portions as permitted by § 42.24(a).

Date: 11/20/2024

/Joshua D. Curry/