

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.
Petitioner,

v.

UMBRA TECHNOLOGIES LTD
Patent Owner.

U.S. Patent No. 10,630,505
Issue Date: April 21, 2020
Title: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

Inter Partes Review No.: IPR2024-00497

**PETITION FOR *INTER PARTES* REVIEW OF PATENT NO. 10,630,505
UNDER 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.1-.80, 42.100-.107**

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

	Page
I. INTRODUCTION	1
II. OVERVIEW	1
III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A)).....	6
IV. REASONS FOR THE REQUESTED RELIEF	6
A. Summary of the '505 Patent.....	6
B. Prosecution History	13
C. Claim Construction.....	15
D. Priority Date of the Challenged Claims	16
E. Person of Ordinary Skill in the Art	16
F. State of the Art	17
1. Communication Tunnels	17
2. Selection of Communication Paths By Controller	19
3. DNS Look Ups	20
4. Caches	20
V. IDENTIFICATION OF CHALLENGES	21
A. Challenged Claims	21
B. Statutory Grounds for Challenges	21
C. Prior Art.....	21
VI. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	23
A. Challenge 1: Claims 1, 2, 4-12, 14-20 are unpatentable over Hankins, alone, or in view of Munger.....	23

1.	The Hankins Reference	23
2.	The Munger Reference	29
3.	Detailed Application of Hankins and Munger To The Challenged Claims	30
B.	Ground 2: Claims 3 and 13 are unpatentable over Hankins, alone or in view of Munger, in further view of Treuhaft,.....	66
1.	The Treuhaft Reference	66
2.	Detailed Application Of Hankins, Munger And Treuhaft To Claims 3 And 13	67
VIII.	Mandatory Notices Under 37 C.F.R. §42.8.....	74
A.	Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)).....	74
B.	Related Matters (37 C.F.R. § 42.8(b)(2)).....	74
1.	Judicial Matters	74
2.	Administrative Matters:	75
3.	Related Patents.....	75
C.	Lead/Back-up Counsel (37 C.F.R. § 42.8(b)(3)):	75
D.	Notice of Service Information (37 C.F.R. § 42.8(b)(4)):.....	76
IX.	CONCLUSION.....	76

Petitioner's Exhibit List

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 10,630,505 (the "'505 Patent")
1002	Select portions of prosecution history of the '505 Patent ("File History")
1003	Declaration of Petitioner's Expert Dr. A.L. Narasimha Reddy ("Reddy")
1004	U.S. Patent No. 10,177,957 ("Hankins")
1005	U.S. Patent No. 6,502,135 ("Munger")
1006	U.S. Pat. App. Publ. No. 2014/0359704 to Chen ("Chen")
1007	U.S. Pat. App. Publ. No. 2010/0275017 to Iyer ("Iyer")
1008	RFC 1034 (November 1987) ("Mockapetris")
1009	U.S. Pat. App. Publ. No. 2013/0275570 to Treuhaft et. al. ("Treuhaft")
1010	Related Patents
1011	Computer Networks

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311 *et seq.* and 37 C.F.R. §§ 42.1 *et seq.*, Cisco Systems, Inc. (“Petitioner”) hereby petitions for an *inter partes* review of U.S. Patent No. 10,630,505 (the “’505 Patent”). Petitioner respectfully submits that Claims 1-20 (the “Challenged Claims”) of the ’505 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art references discussed herein. This Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of these claims. Accordingly, it is respectfully requested that the Board institute an *inter partes* review of the ’505 Patent pursuant to 37 C.F.R. § 42.108.

II. OVERVIEW

The Challenged Claims are unpatentable as obvious over the prior art. The claims are directed to prior art systems and combinations of conventional components that perform conventional functions regarding network routing and network services, all of which were well-known in the art of network communications.

Specifically, the Challenged Claims are directed to a system (Claims 1-10 and 14-20) and method (Claims 11-13) for connecting devices via a network comprising two end point devices (EPD), a plurality of access point servers (SRV_AP) that form a plurality of end-to-end tunnels connecting the two devices,

and a control server (SRV_CNTRL) that selects one of the plurality of end-to-end tunnels for communication between the two devices. The '505 Patent provides FIG. 23 as illustrating one example of the multiple end-to-end tunnel connectivity between end point devices:

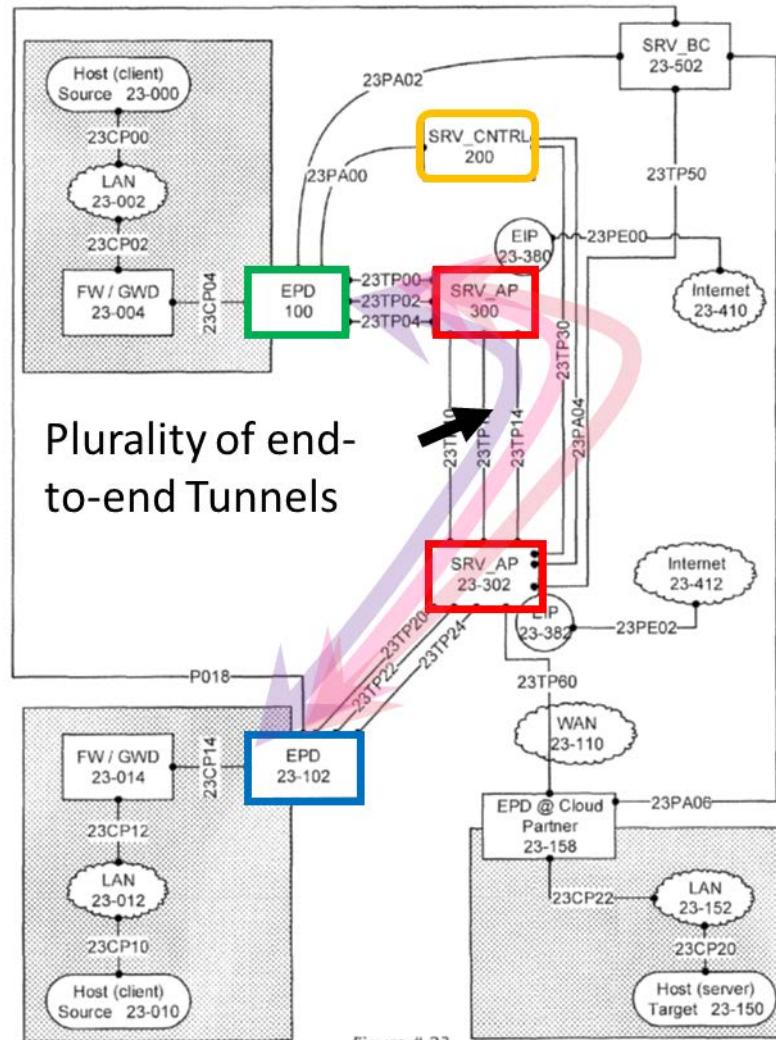


Figure # 23

EX-1001 Fig. 23; EX-1003 ¶28.

The '505 Patent describes the system as comprising a first device EPD 100 (green) and a second device EPD 23-102 (blue), a plurality of intermediate access

point servers SRV_AP 300 (**red**) and SRV_AP 23-302 (**red**) that form a plurality of end-to-end tunnels (**purple/pink/mauve**), and a central server SRV_CNTRL 200 (**gold**) that selects one of the end-to-end tunnels for communication between the devices based upon information the central server receives from at least one of the access point servers. EX-1003 ¶29.

Specifically, Claim 1 (representative of independent Claims 11 and 14) recites:

*1. A network system comprising:
a first device;
a second device; and
a plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first device and the second device; and
a control server, wherein the control server receives information from at least one of the plurality of intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information.*

EX-1001 Claim 1

However, a comparison of U.S. Patent No. 10,177,957 (“Hankins”)(EX-1004) to the Challenged Claims demonstrates that the system and method recited in the Challenged Claims were well-known prior to the purported invention of the ’505 Patent. Although Hankins provides a parallel disclosure to the ’505 Patent,

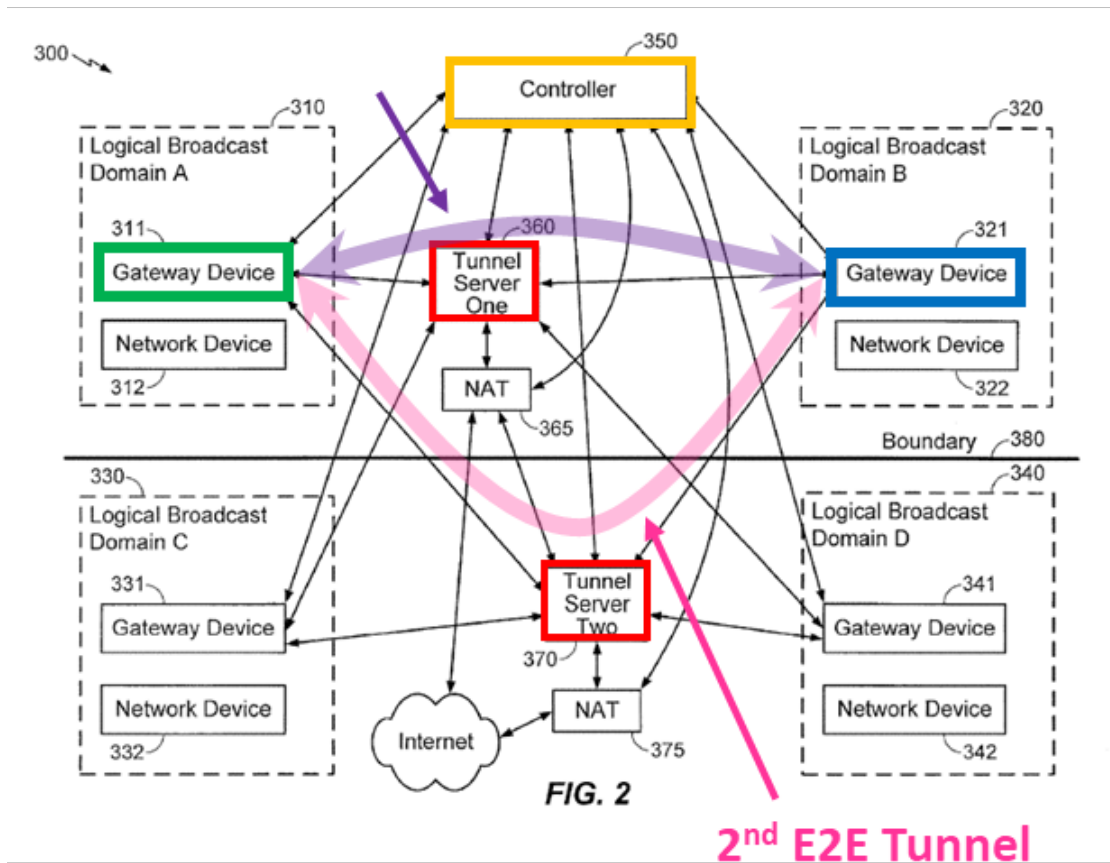
Hankins uses different terminology. A mapping of the terminology used in the '505 Patent and Hankins is provided below:

Claim 1 recited terms	'505 Patent	Hankins
<i>a first device</i>	EPD 100	Gateway Device 311
<i>a second device</i>	EPD 23-102	Gateway Device 321
<i>a plurality of intermediate access point servers</i>	SRV_AP 300 SRV_AP 23-302	Tunnel Server One 360 Tunnel Server Two 370
<i>a plurality of end-to-end tunnels</i>	Tunnels 23TP (00, 02, 04) + (10, 12, 14) + (20, 22, 24)	1 st tunnel and 2 nd tunnel between Gateway devices
<i>a control server</i>	SRV_CNTRL 200	Controller 350

EX-1003 ¶ 31.

The embodiment disclosed by Hankins in FIG. 2 is shown below and has been annotated to show the elements recited in Claim 1:

1st E2E Tunnel



EX-1004 Fig. 2; EX-1003 ¶32.

Hankins discloses the system illustrated in FIG. 2 includes a first gateway device 311 (**green**) and a second gateway device 321 (**blue**), a plurality of access point servers including tunnel server one (**red**) and tunnel server two (**red**) that each form an end-to-end tunnel (**purple** and **pink**) between the devices, and a central server controller 350 (**gold**) that selects one of the end-to-end tunnels for communication between the devices based upon information the controller 350 receives from at least one of the tunnel servers. EX-1004 Fig. 2; EX-1003 ¶33.

Hankins demonstrates that the purported invention recited in the Challenged Claims was well-known at the time of the '505 Patent and is unpatentable as set forth below in Grounds 1 and 2. Secondary references Munger and Treuhaft are cited to demonstrate that the features recited in the dependent claims directed to domain name service functionality were also well-known.

III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A))

Petitioner certifies that the '505 Patent for which review is sought is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review of the Challenged Claims on the grounds identified herein. 37 C.F.R. § 42.104(a). This Petition is filed pursuant to 37 C.F.R. § 42.106(a).

IV. REASONS FOR THE REQUESTED RELIEF

As explained in §§ II and VI-VIII of this Petition and in the attached Declaration of Petitioner's Expert, Dr. A.L. Narasimha Reddy ("Reddy"), *EX-1003*, the systems and methods of connecting different networks via tunneling, as described and claimed in the '505 Patent, were obvious over the prior art to a person of ordinary skill in the art ("POSITA") at the time of the invention.

A. Summary of the '505 Patent

The '505 Patent is directed to managing a network connection between network devices and an access point server. The '505 Patent discloses as a problem that in the prior art there is insufficient control over the routes between a

network device and access point server as it relies on the policies of various middle players on the Internet who carry the traffic over their networks and peer to other carriers or network operators. EX-1001 2:48-59; EX-1003 ¶36.

The '505 Patent describes that it is not uncommon to connect from within one local area network (LAN) to the resources of another LAN using a direct connection through a wide area network (WAN), such as the Internet. However, the '505 Patent describes a problem that arises when a gateway to the Internet is located at the LAN of one end, say at the corporate headquarters, which handles traffic from a remote LAN of a subsidiary located in a different country. A slowdown occurs as traffic flows from the remote LAN through the WAN to the LAN where the gateway is located and then through the Internet back to a server in the origin country, then back through the Internet to the gateway, and then back down the dedicated line to the client device within the LAN. This type of connection in essence doubles or triples (or worse) the global transit time of what should take a small fraction of global latency to access this nearby site. Thus, the prior art connection mechanisms may not take into account the context of the connection needed for a particular source endpoint device and available access point servers. EX-1001 2:31-2:47; EX-1003 ¶37.

As a solution, the '595 Patent describes a cloud based solution for establishing dedicated connections between network devices and an access point

server. EX-1001 2:40-57. The '505 Patent describes systems and methods for connecting endpoints via first and second devices that are connected by a communication path composed of one or more intermediate tunnels connecting each endpoint device to one or more intermediate access point servers and one or more control servers. EX-1001 Abstract; EX-1003 ¶38.

The '505 Patent provides FIG. 23 as illustrating multiple tunnel connectivity between end point devices (EPD) and intermediate access point servers (SRV_AP). The tunnels can be used for client data traffic, internal system data or other transfers. FIG. 23 further demonstrates the connecting of infrastructure devices such as central server (SRV_CNTRL) 200 and back channel admin server (SRV_BC) 23-502 with other devices.

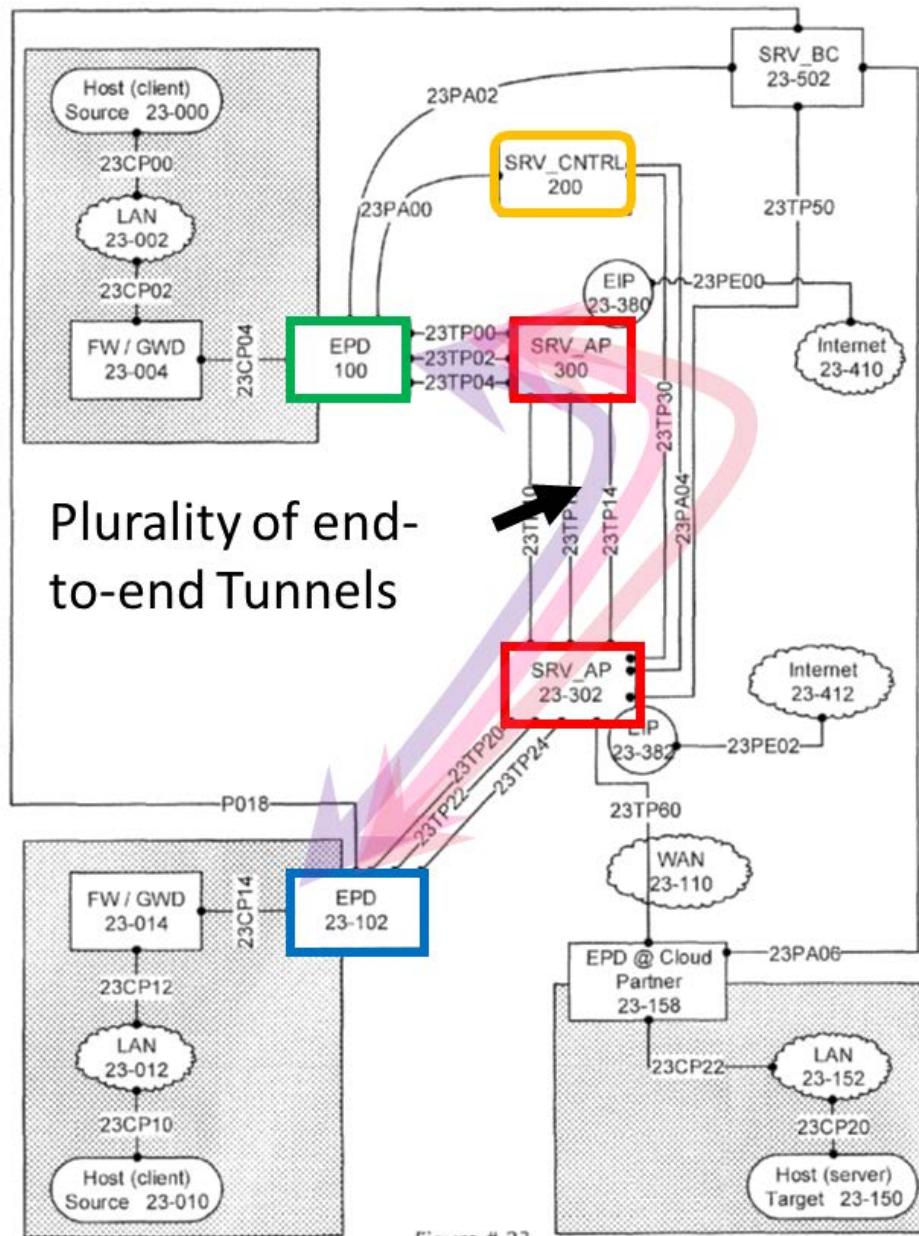


Figure # 23

EX-1001 Fig. 23; EX-1003 ¶39.

With reference to FIG. 23, the '505 Patent describes the system as comprising a first device EPD 100 (green) and a second device EPD 23-102 (blue), a plurality of intermediate access point servers (SRV_AP 300 (red) and

SRV_AP 23-302 (**red**)). Between each of the EPDs and access point servers are a plurality of tunnels. Each of these individual tunnels can be combined in various combinations to form a plurality of end-to-end tunnels (**purple/pink/mauve**) between EPD 100 and EPD 23-102. A central server SRV_CNTRL 200 (**gold**) selects each of the individual tunnels to form an end-to-end tunnel for communication between the devices based upon information the central server receives from at least one of the intermediate access point servers. EX-1001 23:55-64; EX-1003 ¶40.

End point device EPD 100 (**green**) can connect LAN 23-002 to access point server SRV_AP 300 (**red**) via tunnel 23TP00, 23TP02 or 23TP04. Internet. EX-1001 24:5-9; EX-1003 ¶41.

End point device EPD 23-102 (**blue**) can connect LAN 23-012 to access point server SRV_AP 302 (**red**) via tunnel 23TP20, 23TP22 or 23TP24. Internet. EX-1001 24:13-14; EX-1003 ¶42.

The access point servers (**red**) SRV_AP 300 and SRV_AP 302 are connected via tunnel 23TP10, 23TP12 or 23TP14. EX-1001 24:10-12; EX-1003 ¶43.

Thus, a plurality of end to end tunnels can be formed between endpoint devices 100 and 23-102 based on various combinations of individual tunnels through access point server 300 and 23-302. EX-1001 24:33-39; EX-1003 ¶44.

The '505 Patent describes forming end-to-end tunnels (purple/pink) between the EPDs via one intermediate access point server (red) as illustrated in FIG. 33 below:

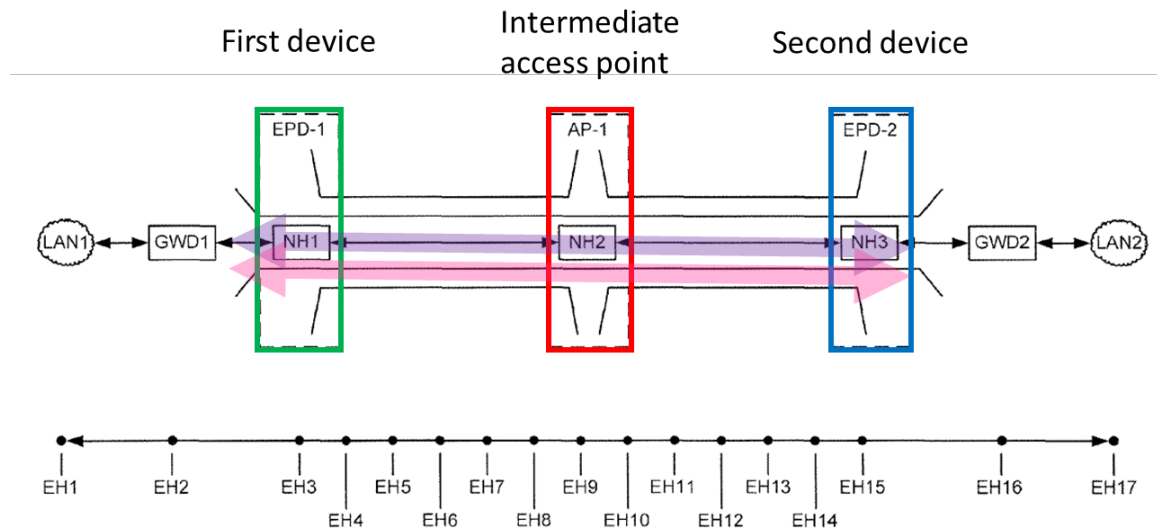


Figure # 33

EX-1001 FIG. 33, 33:8-16; EX-1003 ¶45.

The '505 Patent also describes forming end-to-end tunnels (purple/pink) between the EPDs via more than one intermediate access point server (red) as illustrated in FIG. 34 below:

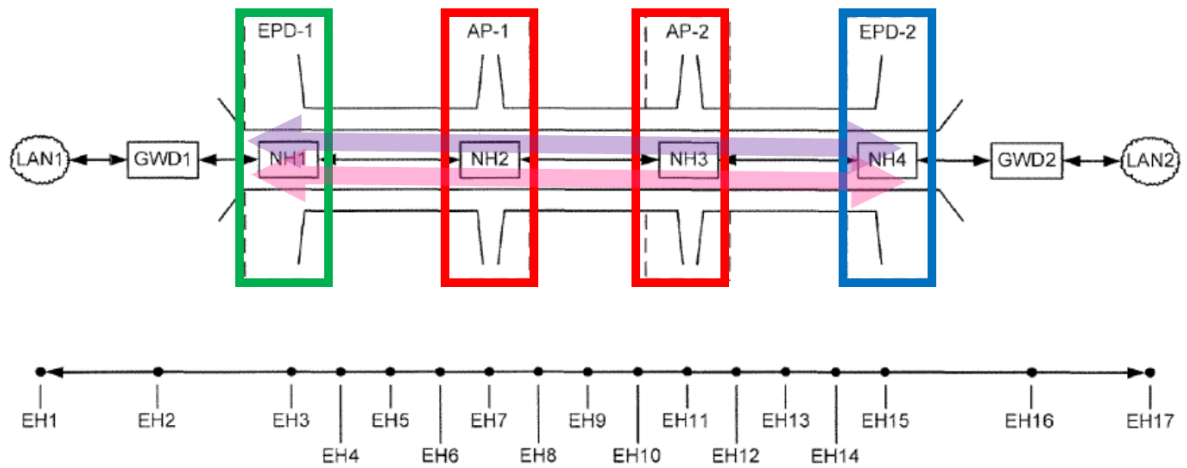


Figure # 34

EX-1001 FIG. 34, 33:25-31; EX-1003 ¶46.

The '505 patent also describes the Local DNS server and cache 154 on EPD 100 and 354 on SRV_AP 300 allows for caching of DNS lookups for fast, local retrieval. EX-1001 19:24-26; EX-1003 ¶47.

The '505 Patent includes twenty claims with Claim 1 (network system), Claim 11 (method) and Claim 14 (system) being independent. Claim 1 is representative:

[1.0] *A network system comprising:*

[1.1] *a first device;*

[1.2] *a second device; and*

[1.3] *a plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first device and the second device; and*

[1.4] *a control server, wherein the control server receives information from at least one of the plurality of intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information.*

B. Prosecution History

The Office rejected Claims 1-4 and 8-9 as being anticipated by Chen, and Claims 5-7 as being obvious over Chen in view of TW Telecom.

In response, Applicant amended the claims as follows:

1. (Currently amended) A network system ~~for connecting devices via a global virtual network,~~ comprising:
 - a first device ~~in communication with a first endpoint device;~~
 - a second device ~~in communication with a second endpoint device;~~ and
 - a ~~communication path~~ plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first ~~device~~ and the second ~~end-point~~ device; and
 - a control server, wherein the control server receives information from at least one of the plurality of intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information

~~further comprising one or more intermediate tunnels connecting each endpoint device to one or more intermediate access pointer servers and one or more control servers.~~

EX-1002 145

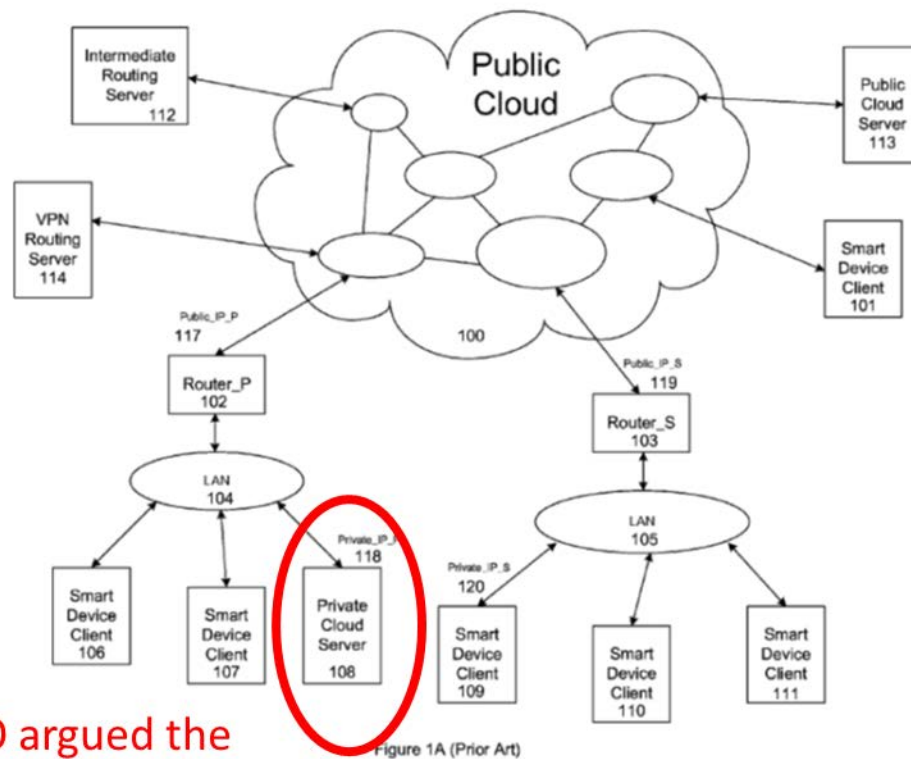
Applicant argued that Chen does not teach:

1) a plurality of end-to-end tunnels connecting the first device and the second device;

2) nor a control server;

as recited in amended Claim 1. EX-1002 150.

Applicant argued further that Chen only describes tunnels “between the smart device client 109 and the private cloud server 108” and does not disclose tunnels “between pairs of Smart Device Clients 101, 107, or 109.” EX-1002 151. Applicant specifically noted, “Chen does not teach that the Private Cloud Server 108 joins multiple VPN links to provide end-to-end encapsulation and consequently the VPN links would not form a ‘plurality of end-to-end-tunnels.’”



PO argued the
Cloud Server 108
does not join
VPN links

EX-1006 FIG. 1A (annotated).

In response and without comment the Office allowed the application and it issued as the '505 Patent with Claims 1-20. EX-1002 22-25.

C. Claim Construction

Petitioner proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction.

It is noted that this interpretation is only applicable to the *inter partes* review sought herein and should not be construed as constituting, in whole or in part, Petitioner's own interpretation of any claims for any other purposes, including any litigation. Accordingly, Petitioner expressly reserves the right to present an interpretation of a claim term in other proceedings, which is different, in whole or in part, from that presented in this Petition.

D. Priority Date of the Challenged Claims

The application that issued as the '505 Patent was filed Jul. 25, 2017 as a 371 national stage of PCT application PCT/US2016/015278 claiming priority to two PCT applications filed, Jan. 5, 2016 and Dec. 7, 2015, and multiple provisional applications, the earliest of which was filed on Jan. 28, 2015. For purposes of this Petition, Petitioner assumes the earliest possible priority date of Jan. 28, 2015

E. Person of Ordinary Skill in the Art

With respect to the '505 Patent, a POSITA in 2015 would have been familiar with network communications including virtual private networks and interconnections therebetween. EX-1003 ¶ 53. A POSITA would have a working knowledge of techniques for transmitting data via a VPN and establishing tunneling links. A POSITA would have gained knowledge of these concepts through a mixture of training and work experience, such as by having a Bachelor's degree in computer science and four years of experience; or by obtaining a

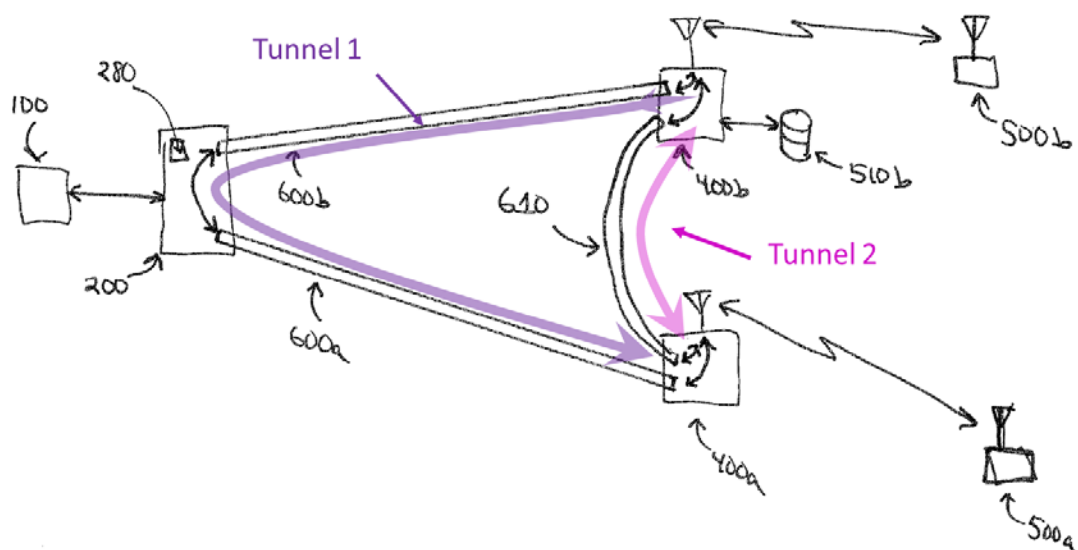
Master's degree in computer science, but having only one to two years of experience; or by having no formal education but experience in storage systems of at least eight years. EX-1003 ¶ 53.

F. State of the Art

The following section describes the state of the art for network communications as of the priority date of the '505 Patent. EX-1003 ¶55. The prior art references, and the discussions of what was known to a POSITA, provide the factual support for the general description of the state of the art at the time of the invention, and provide additional motivation to modify or combine the references. Accordingly, these references should be considered by the Board.

1. Communication Tunnels

The use of “tunnels” was well known in the art. For example, Iyer (2010) disclosed a plurality of communication paths (**tunnel 1** and **tunnel 2**) between wireless clients, which were identified as “peer-to-peer tunnels” established between “any two clients in the mobility domain” to route traffic between the clients. Traffic between the clients pass through the tunnels and intermediate access point servers. EX-1007, [0015, 30]; EX-1003 ¶ 56.



EX-1007 Fig. 4; EX-1003 ¶ 56.

The two communication paths connecting wireless clients 500a and 500b are “form[ed]” by access nodes 400a and 400b, because access nodes 400a and 400b “establish” the tunnel 610, or tunnels 600a and 600b.

[M]obility manager 280 instructs access node 400a to establish peer-to-peer tunnel 610 between access node 400a and access 400b.

EX-1007 [0030]; EX-1003 ¶ 56.

[T]he access nodes establish communications with the controller using tunnels.

EX-1007 [0013]; EX-1003 ¶ 56.

2. Selection of Communication Paths By Controller

It was well known in the art to provide a controller that selected the communication path, including the selection of tunnels, between client devices. For example, Iyer discloses that the Controller 200 identifies the traffic destination and selects the tunnel through access nodes that the traffic uses. EX-1007, [0025. 26]; EX-1003 ¶ 57.

Iyer describes a controller establishes peer-to-peer tunnels between access nodes to route that traffic between the clients. EX-1007 [0030]; EX-1003¶ 58.

This routing is performed by controller 200 using the IP addresses of clients 500a and 500b, as well as the MAC (media access controller) addresses of clients 500a, 500b and access nodes 400a and 400b.

EX-1007 [0026]; EX-1003 ¶ 58.

When client 500a wishes to send data to client 500b, it in essence forms an IP packet with client 500b's IP address as the destination, and with client 500a's IP address and MAC address as the source. This information is encapsulated and sent to controller 200.

EX-1007 [0026]; EX-1003 ¶ 58.

Controller 200 identifies the traffic destination as client 500b, and sends the traffic though tunnel 600b to access node 400b and client 500b.

Ex-1007 [0026]; EX-1003 ¶ 58.

3. DNS Look Ups

Domain Name Service (DNS) requests performed at network devices as well as caching those request were also well known. EX-1011 pp. 622-633. For example, Chen discloses a smart device client is configured to perform a DNS lookup to locate a second Smart Device Client by logging into the VPN Routing Server 114 and looking up the virtual IP address of the Private Cloud Server 108. EX-1006 [0055]; EX-1003 ¶59.

4. Caches

In order to obtain information over networks including DNS information, it was well known to implement caches of information previously retrieved, or store requests for further processing. DNS caching was well known basic textbook knowledge (“Computer Networks: a Systems Approach” EX-1011 pp. 622-633) and a POSITA understood that DNS servers cached recent name resolutions until a TTL (Time To Live) expires. For example Mockapetris (1987) disclosed caching information at name servers for fast, local retrieval. EX-1008 12-13, 29, 33; EX-1003 ¶61.

Mockapetris describes that when a request is received, a first step is checking if the requested content is in the cache: “Step 1 searches the cache for the desired data. If the data is in the cache, it is assumed to be good enough for normal use.” EX-1008 34; EX-1003 ¶62.

A POSITA understood that caches and the use of caches in networks were well known as of the filing date of the '505 Patent. EX-1003 ¶63.

V. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 1-20 of the '505 Patent are challenged in this Petition.

B. Statutory Grounds for Challenges

The Challenges are set forth in detail below and summarized as follows:

Ground	Claims	Basis	Reference
1	1, 2, 4-12, 14-20	§ 103	Hankins, alone, or in view of Munger
2	3 and 13	§ 103	Hankins, alone, or in view of Munger, or further in view of Treuhaft

Ground 1: Claims 1, 2, 4-12, 14-20 of the '505 Patent are unpatentable over Hankins, alone, or in view of Munger.

Ground 2. Claims 3 and 13 of the '505 Patent are unpatentable over Hankins, alone, or in view of Munger, or in further view of Treuhaft.

C. Prior Art

1. The Hankins Reference

U.S. Patent 10,177,957 ("Hankins") (EX-1004) is titled CONNECTING A CLOUD NETWORK TO THE INTERNET and issued Jan 8, 2019 from an application filed Mar. 13, 2013. Hankins qualifies as prior art under AIA

§102(a)(2). Hankins was not cited or applied by the Office during prosecution of the Challenged Claims.

2. The Munger Reference

U.S. Patent No. 6,502,135 (“Munger”) (EX-1005) is titled AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY and issued Dec. 31, 2002 from an application filed Feb. 15, 2000, claiming priority to Oct 30, 1998. Munger qualifies as prior art under §102(a)(1). Munger was not cited or applied by the Office during prosecution of the Challenged Claims.

3. The Treuhaft reference

U.S Patent Application Publication No 2013/0275570 (“Treuhaft”) (EX-1009) is titled CROSS-PROTOCOL COMMUNICATION IN DOMAIN NAME published Oct. 17, 2013 from an application filed Apr. 16, 2012. Treuhaft qualifies as prior art under §102(a)(1). Treuhaft was not cited or applied by the Office during prosecution of the Challenged Claims.

VI. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

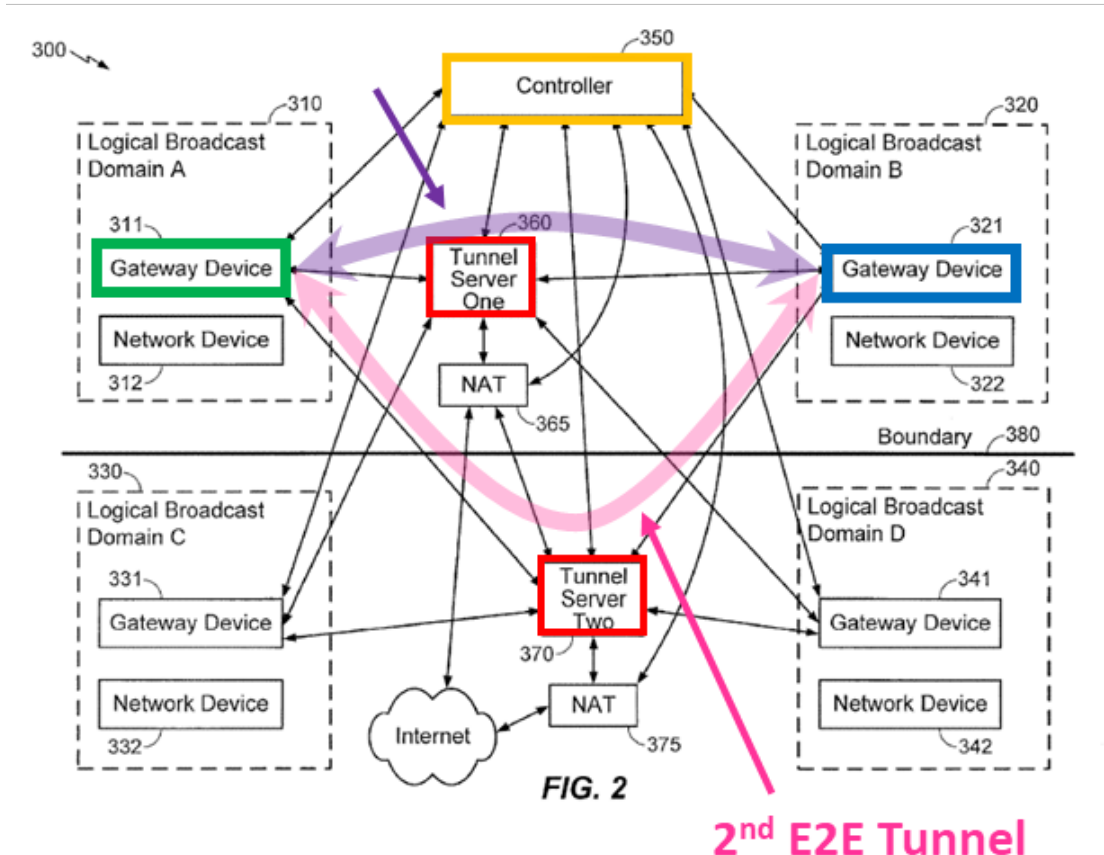
A. Challenge 1: Claims 1, 2, 4-12, 14-20 are unpatentable over Hankins, alone, or in view of Munger

1. The Hankins Reference

Hankins describes managing networks, including connecting a private network to the Internet and communicating signal packets from a first device in a first logical broadcast domain to another network device in another logical broadcast domain as if the logical broadcast domains are not separate. The selected signal packets are transmitted between the network devices of separate logical broadcast domains via a tunnel server. EX-1004 Abstract; EX-1003 ¶¶66. Hankins describes that broadcast domain refers to a set of devices occupying a network address space, in which any device is able to communicate with any other device in the broadcast domain without rerouting a transmission. EX-1004 6:33-40; EX-1003 ¶¶67. A logical broadcast domain means that portions of the broadcast domain may not be entirely related to a particular set of devices. EX-1004 7:45-50; EX-1003 ¶¶68.

As shown below Hankins connects the network devices via one or more tunnel servers (**red**). The tunnel servers facilitate connections between a gateway device (**green**) in the first virtual domain with another gateway device (**blue**) in a second virtual domain:

1st E2E Tunnel



EX-1004 FIG. 2; EX-1003 ¶69.

Hankins identifies the same contextual problem identified in the '505 Patent—that prior art tunnel controllers did not take into consideration contextual information regarding the network, such as the location of a tunnel server's location relative to the gateways. Like the '505 Patent, Hankins proposes that the communication channel may be enhanced by using this contextual information, such as by provisioning a tunnel server located more physically proximate to

endpoints. EX-1004 25:7-25; EX-1003 ¶70. Like the '505 Patent, Hankins discloses that the controller may generate a list of available tunnel servers based at least in part on a host of considerations, such as, for example, cost, capability, efficiency, compatibility, resources, proximity, latency, bandwidth (e.g., throughput), utilization, others or combinations thereof. EX-1004 26:55-65; EX-1003 ¶71.

Hankins discloses the system illustrated in FIG. 2 includes a first gateway device 311 (**green**) and a second gateway device 321 (**blue**), a plurality of access point servers including tunnel server one (**red**) and tunnel server two (**red**) that each form an end-to-end tunnel (use two colors **purple**) between the devices, and a central server controller 350 (**gold**) that selects one of the end-to-end tunnels for communication between the devices based upon information the controller 350 receives from at least one of the tunnel servers. EX-1004 Fig. 2; EX-1003 ¶72.

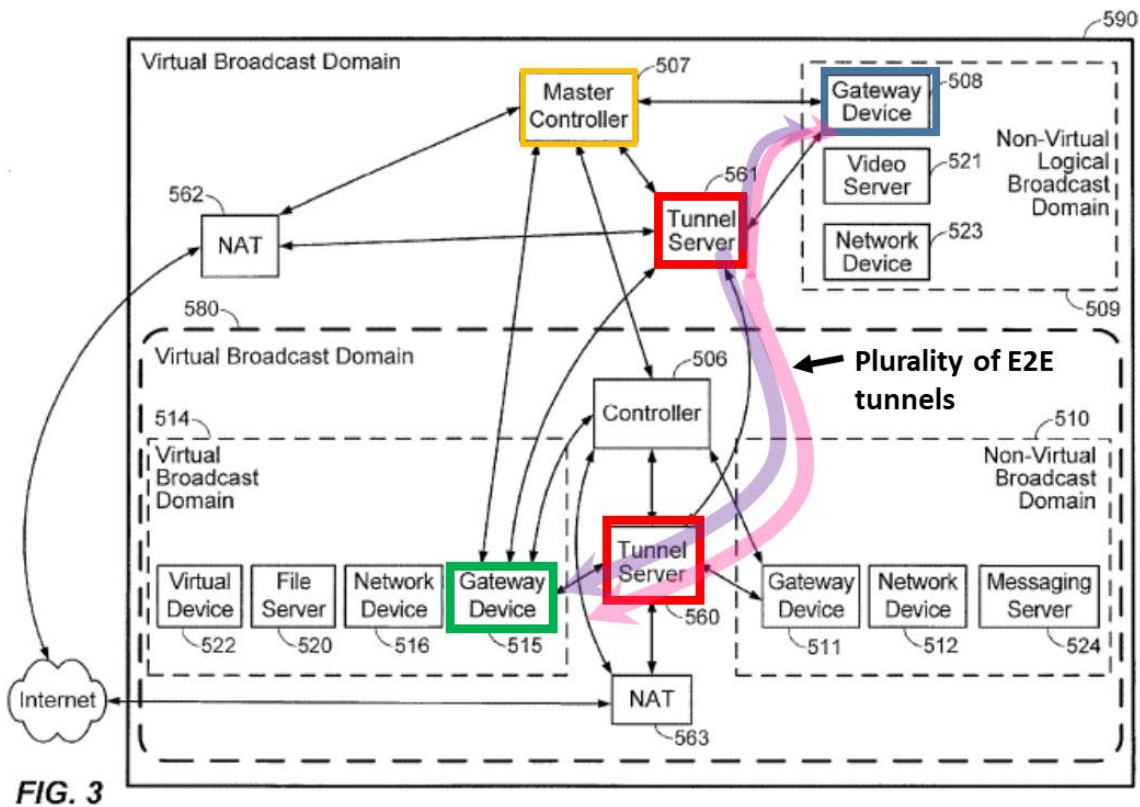
The controller 350 provisions tunnel servers and their respective communication paths depending upon conditions:

[A] controller may provision one or more tunnel servers, for example, to facilitate communications between network devices communicating as part of different broadcast domains.

EX-1004 8:63-66; EX-1003 ¶73.

Hankins describes a variety of factors or considerations for provisioning tunnel servers, including available bandwidth, latency, network utilization or performance and cost. EX-1004, 25:34-55; EX-1003 ¶74.

Like the '505 Patent, Hankins also describes forming a plurality of end-to-end tunnels between two EPDs via one intermediate access point server or more than one intermediate access point server. As illustrated in FIG. 3 below, Hankins describes that a plurality of end-to-end tunnels (**purple and pink**) between gateway device 515 (**green**) and gateway device 508 (**blue**) via only tunnel server 561 (**red**) (i.e., the first E2E tunnel (purple)labeled below) or via tunnel servers 560, 561 (i.e., the second E2E tunnel(pink) labeled below). EX-1004 32:47-60; EX-1003 ¶75.



EX-1004 FIG. 3; EX-1003 ¶75.

Additionally, although FIGs. 2 and 3 of Hankins show a single line between the gateway devices and tunnel servers, Hankins describes these devices are logically joined such that a POSITA understood that the lines represent multiple tunnel paths between the gateway devices and tunnel servers. EX-1004 7:56-65; 36:18-27 (“a tunneling protocol may be substantially compliant with ... Multipath Virtual Private Network”) ; EX-1003 ¶76. Thus, with reference to FIG. 2, a POSITA understood that the single line between gateway 311 and gateway 321 through tunnel server 360 represents a plurality of end-to-end tunnels and likewise,

the single line between gateway 311 and gateway 321 through tunnel server 370 represents a plurality of end-to-end tunnels. The tunnels are selected by the controller 350 (**gold**) using information obtained from the network devices (gateway, tunnel servers, etc.). EX-1004 24:39-57, 25:15-55; EX-1003 ¶77.

FIG. 4 of Hankins generally illustrates the process and tasks of the gateways (**green**), controller (**gold**) and tunnel servers (**red**) in establishing the communication paths and transmitting packets.

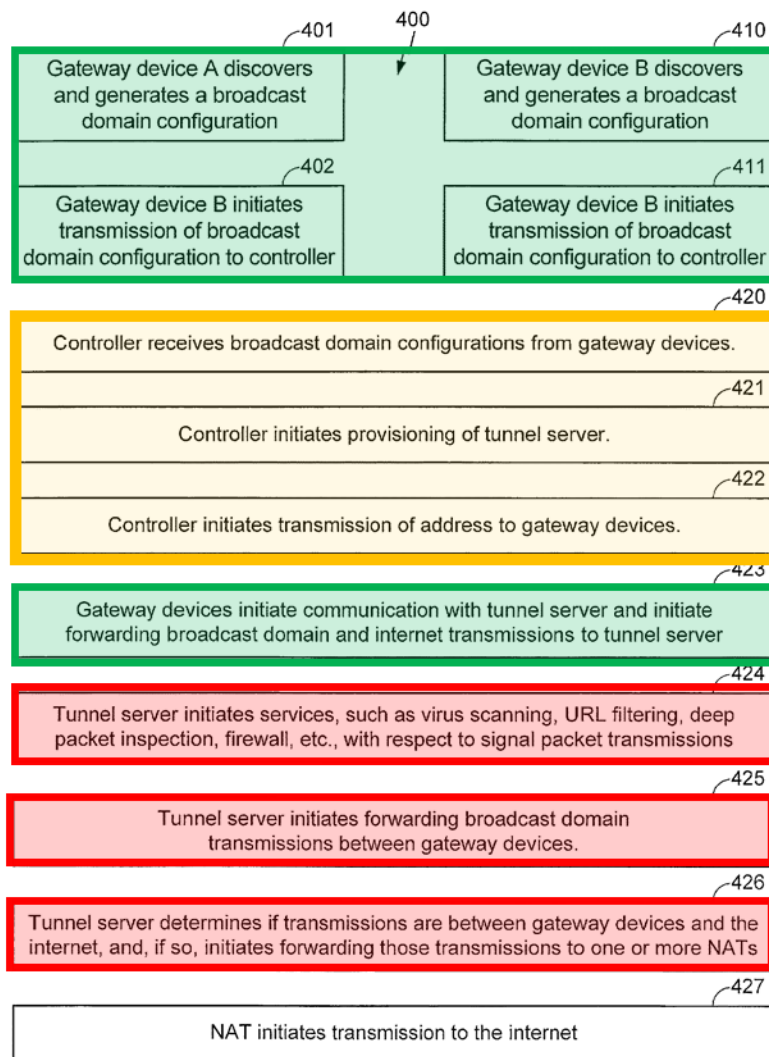


FIG. 4

EX-1004 FIG. 4; EX-1003 ¶ 78.

2. The Munger Reference

Munger is directed to a domain name server that receives a request from a client computer for an IP address corresponding to a domain name associated with a destination computer. Munger discloses a plurality of computer nodes that communicate using seemingly random Internet Protocol source and destination addresses. Packets matching criteria are accepted for further processing, while

those that do not are rejected. Munger discloses a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry. EX-1005 Abstract; EX-1003 ¶79.

Munger discusses a client computer performs a DNS lookup, e.g., by sending a DNS lookup request to locate a target computer:

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

EX-1005 47:20-33); EX-1003 ¶80.

Munger further teaches a DNS server that “provide[s] a look-up function that returns the IP address of a requested computer or host.” EX-1005 37:22-24; EX-1003 ¶81.

3. Detailed Application of Hankins and Munger to the Challenged Claims

Claim 1

[1.0] *A network system comprising*

Hankins discloses a network [*network system*] that communicates packets from one network device to another.

Furthermore, the at least one private network communicates selected signal packets from at least one network device in one of at least two separate logical broadcast domains transmitted to at least one network device in another of at least two separate logical broadcast domains as

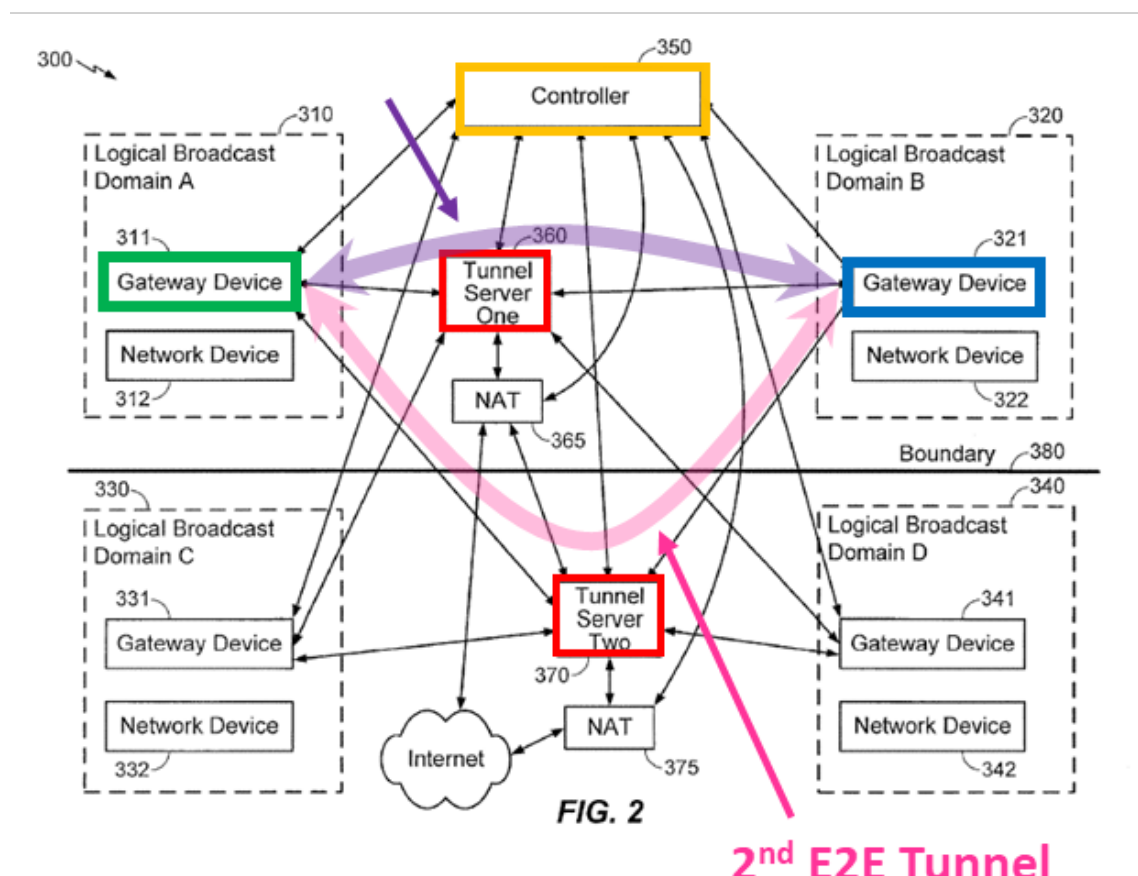
if the logical broadcast domains are not separate. The selected signal packets are transmitted between the network devices of the at least two separate logical broadcast domains via a tunnel server.

EX-1004 Abstract; EX-1003 ¶ 82.

[1.1] *a first device*

Hankins discloses a gateway device 311 (**green**) [*first device*] in a first logical broadcast domain in a network. EX-1004 24:39-57; EX-1003 ¶83.

1st E2E Tunnel



EX-1004 FIG. 2¹ ; EX-1003 ¶83.

[1.2] *a second device*

Hankins discloses a gateway device 321 (**blue**) [*second device*] in a second domain in the private network as shown in Annotated FIG. 2 above. EX-1004 24:39-57; EX-1003 ¶84.

[1.3] *a plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first and the second device*

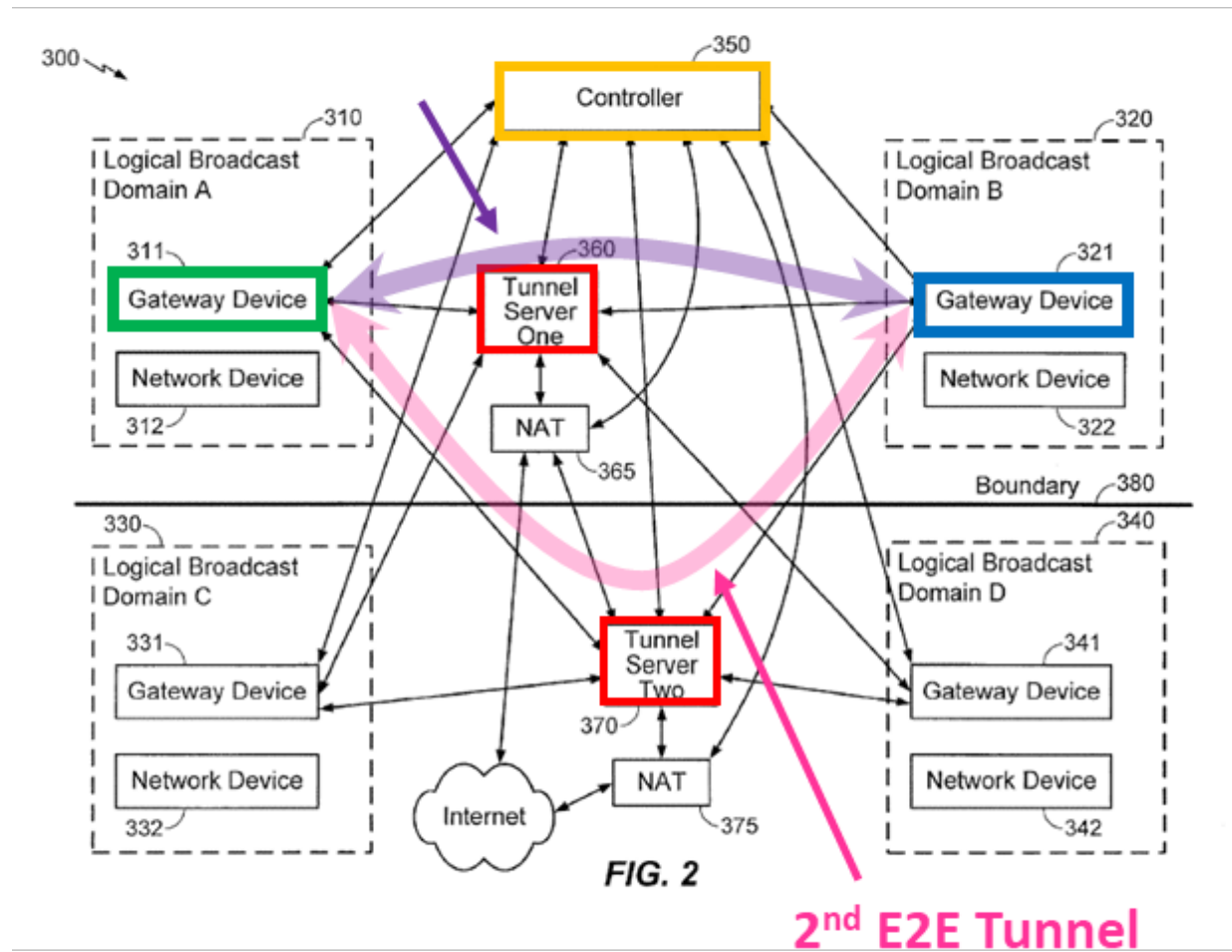
Hankins provides several examples disclosing this limitation.

For example, FIG. 2 shows a first end-to-end tunnel (**purple**) between gateway 311 and gateway 321 through tunnel server 360, and a second end-to-end tunnel (**pink**) between gateway 311 and gateway 321 through tunnel server 370. Thus, FIG. 2 discloses tunnel servers 360 and 370 (*a plurality of intermediate access point servers*) that form a first end-to-end tunnel from gateway 311 to gateway 321 through tunnel server 360, and form a second end-to-end tunnel from gateway 311 to gateway 321 through tunnel server 370 (*a plurality of end-to-end tunnels connecting the first and the second devices*). EX-1004 25:14-33, FIG. 2;

¹ This annotation of FIG. 2 of Hankins will be referred to as “Annotated FIG. 2” in the application of Hankins to the Challenged Claims in Grounds 1 and 2.

EX-1003 ¶86.

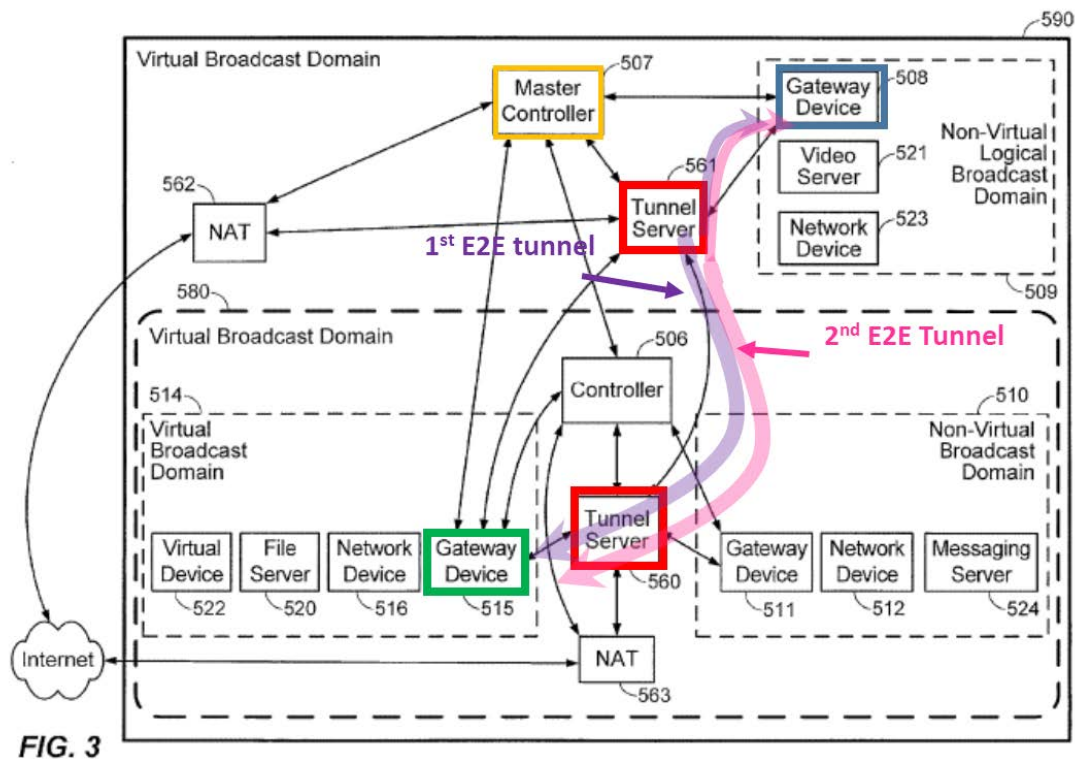
1st E2E Tunnel



EX-1004 FIG. 2; EX-1003 ¶86.

To the extent that PO asserts that each end-to-end tunnel is required to pass through a plurality of intermediate access point servers, Hankins provides another embodiment in FIG. 3 that discloses a plurality of end-to-end tunnels passing through tunnel servers 560 and 561. In FIG. 3, Hankins illustrates tunnel servers 560, 561 [*a plurality of intermediate access point servers*] that form a plurality of

end-to-end tunnels. For example a first end-to-end tunnel connects gateway device 515 (**green**) [*first device*] with gateway device 508 (**blue**) [*second device*] via tunnel server 561 and 560 and a second end-to-end tunnel via tunnel server 561 and tunnel server 560. EX-1004 32:47-60, FIG. 3; EX-1003 ¶87.



EX-1004 FIG. 3; EX-1003 ¶87.

In a further example, Hankins discloses tunnel servers 360 and 370 (**red**) [*a plurality of intermediate access point servers*] that form a plurality of paths or channels (**purple**) [*end-to-end tunnels*] connecting the gateway device 311 (**green**) [*first device*] with the gateway device 321 (**blue**) [*second device*] as shown in FIG. 2 below. EX-1003 ¶88. Although FIG. 2 of Hankins shows a single line between

the gateway devices and tunnel servers, Hankins describes these devices are logically joined which a POSITA understood would represent multiple tunnel paths between the gateway devices and tunnel servers. EX-1005 7:56-65; 36:18-27 (“a tunneling protocol may be substantially compliant with ... Multipath Virtual Private Network ”). Thus, a POSITA understood that the single line between gateway 311 and gateway 321 through tunnel server 360 represents a first plurality of end to end tunnels and likewise, the single line between gateway 311 and gateway 321 through tunnel server 370 represents a second plurality of end to end tunnels. EX-1003 ¶90.

1st Plurality of E2E Tunnels

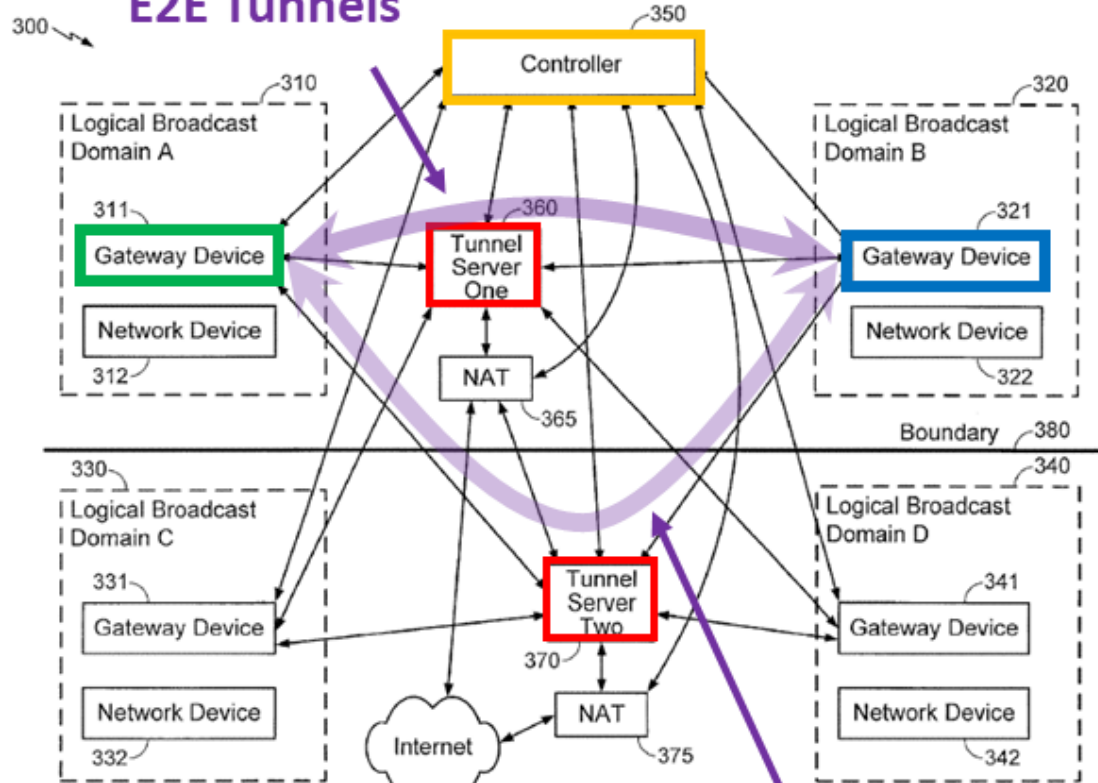


FIG. 2

2nd Plurality of E2E Tunnels

EX-1004 FIG. 2 ; EX-1003 ¶90.

Hankins discloses the use of tunneling protocols to route packets from the first device to the second device:

Tunneled traffic may, or may not be encrypted, and a tunneling protocol may be substantially compliant with and/or substantially compatible with any past, present or future versions of any of the following protocols: IPSec, Transport Layer Security, Datagram Transport Layer Security, Microsoft Point-to-Point Encryption,

Microsoft's Secure Socket Tunneling Protocol, Multipath Virtual Private Network, Secure Shell VPN, another existing protocol, and/or another protocol that may be developed.

EX-1004 36:18-27; EX-1003 ¶91.

Hankins discloses that network devices in separate logical broadcast domains may communicate with and/or via a tunnel server. For example, a tunnel server may forward traffic between gateway devices such as for communications between different logical broadcast domains. EX-1004 12:61-66; EX-1003 ¶92.

Hankins further discloses that the signal packets may be encapsulated, which allows the gateway devices via the tunnel servers to be connected/linked across domains via the paths or channels:

Thus, for example, if a virtual broadcast domain provides a signal packet A to a tunnel server, it may be encapsulated....a tunnel server may likewise remove encapsulation (e.g., referred to as termination) to determine where to forward a signal packet and re-encapsulate it for forwarding.

EX-1004, 13:8-14; EX-1003 ¶93.

A path or channel for communications may potentially be enhanced by controller 350 provisioning an additional tunnel server located more physically proximate to logical broadcast domain C 330 and logical broadcast domain D 340, for example. Controller 350 may provision tunnel server two 370.

EX-1004 25:15-20; EX-1003 ¶93.

The term tunnel server refers to a mechanism or technique capable of being implemented in a network, such as in software, firmware, hardware or any combination thereof (other than software per se, since software is executed, of course, typically on one or more computing devices), that includes a capability to link logical broadcast domains, such as via encapsulation of signal packets, as previously described,

EX-1004 13:46-54; EX-1003 ¶93.

[1.4] *a control server wherein the control server receives information from at least one of the plurality of intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information.*

Hankins discloses a controller 350 (**gold**) [*control server*] that receives information regarding the network and provisions tunnel servers along with one of the paths or channels [*selects one of the plurality end-to-end tunnels*] for communications between the gateway devices [*first and second devices*] based upon the received information. EX-1004 FIG. 2; EX-1003 ¶94.

In still another possible embodiment, a controller may provision one or more tunnel servers, for example, to facilitate communications between network devices communicating as part of different broadcast domains.

EX-1004 8:63-66; EX-1003 ¶94.

Hankins expressly discloses that signal packets communicated through a tunnel server are a factor for consideration by the controller in provisioning tunnels:

Provisioning an additional tunnel server may be based at least in part on a variety of factors or considerations. For example, signal packets communicated via tunnel server one 360 may be a factor or a consideration.....For example, if available bandwidth decreases, if latency increases, and/or if network utilization increases, controller 350 may provision additional tunnel servers in a manner to improve performance and/or reduce cost without human intervention.

Examples of possible monitoring and / or measurement of network performance and/or cost – related parameter were previously discussed.

EX-1004 25:34-55; EX-1003 ¶95.

For example, in an embodiment, a discovery device may comprise a network device capable of communicating as part of a broadcast domain to discover features of the particular broadcast domain without human intervention to generate a broadcast domain configuration of the particular broadcast domain. A discovery device may engage in a variety of activities to accomplish this including, but not limited to any of the following: passively monitoring signal packets, actively probing other network devices, querying other network devices, querying servers, such as a domain controller or

other server responsible for a directory of broadcast domain features, any combinations thereof, or other approaches.

EX-1004 9:10-22; EX-1003 ¶95.

Hankins includes several examples of the controller selecting one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information:

A path or channel for communications may potentially be enhanced by controller 350 provisioning an additional tunnel server located more physically proximate to logical broadcast domain C 330 and logical broadcast domain D 340, for example. Controller 350 may provision tunnel server two 370.

EX-1004 25:15-20; EX-1003 ¶96.

In an embodiment, tunnel server 560 may be controlled at least in part by a controller 506. For example, tunnel server 560 may be instructed to forward network transmission signal packets from gateway device 515 to gateway device 511, and forward network transmission signal packets from gateway device 511 to gateway device 515, for an embodiment, for example. For an embodiment, gateway device 515 in virtual broadcast domain 514 and gateway device 511 in non-virtual broadcast domain 510 may be linked for at least a period of time, in this example, by tunnel server 560, resulting in a path for signal packet network communications between gateway device 515 and gateway device 511 and thereby forming a virtual BD, at least for a

period of time, so as to forming a secure, private network, for example,

EX-1004 30:15-29; EX-1003 ¶96.

Hankins, while noting that any number of network devices (gateways, tunnel servers, etc.) may collect network data [*information*] used by the controller to select the paths or channels for communications, does not expressly state that the network data [*information*] received by the controller is from the tunnel server [*intermediate access point server*]. However, Hankins describes several examples of information used by the controller to provision tunnels, including “bandwidth decreases,” and “latency increases.” A POSITA understood that signal packets passing through the tunnel servers are identified as factors the controller uses in determining whether to provision an additional path or channels [*select one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information*]. EX-1004 25:34-55; EX-1003 ¶97.

A POSITA understood that the determination of bandwidth decreases or latency increases associated with the tunnel server would be determined from information derived and resident at the tunnel server, and thus received from the tunnel server (directly or indirectly). In addition, Hankins in FIG. 2 illustrates two way communications between the controller 350 and the tunnel servers 360, 370 and the gateway devices 311, 321, 331, 341. Therefore, a POSITA understood

that information related to the signal packets transiting through the tunnel server is transmitted directly or indirectly (via the gateway device) to the controller. EX-1003 ¶100.

While Hankins does not expressly state that the signal packet information received by the controller is directly from the tunnel server, it does describe that discovery devices, including gateways, can monitor signal packets and query other network devices and servers for information that can be used by the controller. EX-1004 9:10-21; 14:33-49. Thus, a POSITA understood that Hankins discloses that the gateway can query a tunnel server for information such as signal packet information and provide this information as part of the configuration information provided by the gateway to the controller. EX-1003 ¶102.

Moreover, Hankins' disclosure is very broad in that it expressly states that a gateway can also function as a tunnel server, and therefore the tunnel server would provide configuration information directly to the controller when the gateway is functioning as a tunnel server. EX-1004 14:40-51 ; EX-1003 ¶103.

To the extent that PO argues that a POSITA would not find an explicit disclosure that the claimed information is received by the controller directly or indirectly from the tunnel server, then it would have been obvious in view of the knowledge of a POSITA. EX-1003 ¶104.

A POSITA understood from the disclosure of Hankins that the desired information may be obtained at the tunnel server, and that the controller of Hankins receives this information and makes path or channel selections based upon this received information. In addition a POSITA understood that Hankins discloses network devices including gateway devices may obtain and provide this information to the controller. Therefore, it would have been obvious to a POSITA to modify Hankins, such that the tunnel server obtains and provides the network information to the controller either directly over the two way communication link, or indirectly through the gateway device. A POSITA would be motivated to make such a modification because:

1) Advantageously, the tunneling server is in possession of the information and is already in communication with the controller;

2) The modification would beneficially reduce the need for another network device to obtain and transmit the network information;

3) Beneficially, the tunneling server would be able to provide real time network information as to signal packets traversing it and its present bandwidth, and latency, both of which are network information desired by the controller in order to select paths and channels between the gateway devices. EX-1003 ¶106.

In addition such a modification would be merely:

4) Simple substitution of one known element for another to obtain predictable results, i.e., the substitution of the tunnel server for the gateway device, or other network device to provide the network information associated with the transient signal packets and involve communicating with the tunnel servers in the same and predictable manner as with the gateway devices;

5) Choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success (“obvious to try”); In Hankins, there are only a finite number of network elements from which the network information could be sent to the controller, including gateway devices, tunnel servers and other network devices. It would have been obvious to select the tunnel server to provide the network information to the controller given the tunnel servers ability to collect the network information, and its two way connection with the controller. Selection of the tunnel servers to provide the network information would have predicable results. EX-1003 ¶107.

A POSITA would also be confident of the success of the combinations because the proposed modification would not result in rearrangement of the network devices, network topology, nor a deviation from their common and intended operation/uses. Allocating tasks among the various network devices was a well understood and predictable endeavor. EX-1003 ¶108.

Claim 2

[2] The network system according to claim 1, wherein at least one of the first device or the plurality of intermediate access point servers is configured to perform a domain name system lookup to locate the second device.

Hankins, alone, or in view of Munger discloses this limitation. Hankins discloses that each of the network devices inclusive of gateways [*first and second devices*] and tunnel servers [*intermediate access point servers*] are configured to provide services, including domain name services/discovery services [*domain name system look ups*] for other network devices such as gateway 321 [*second device*]:

[A] server may provide now known and/or to be later developed, service arrangements, derivatives, and/or improvements, including past, present, and/or future services comprising, but not limited to, web services, third party services, audio services, video services, email services, instant messaging (IM) services, SMS services, MMS services, voice over IP (VOIP) services, calendaring services, photo services, database services, facsimile services, file services, **domain name services**, game services, printing services, proxy services, data streaming services, peer-to-peer services, other services, the like or any combinations thereof.

EX-1004 8:23-33, see also 11:64-12:8; EX-1003 ¶109

At block 424, one or more tunnel servers may receive signal packets and may initiate services. **Services may include**, for example, a private network policy and inspection process, which may include, as examples, virus scanning, filtering (for example, URL filtering), deep packet inspection, a firewall, and others, in connection with processing of the received signal packets.

EX-1004 29:1-8; EX-1003 ¶109.

[A] network device may engage in a variety of activities to accomplish this including, but not limited, to any of the following: passively monitoring signal packets, actively probing other network devices, port scanning other network devices, **querying other network devices, querying servers, such as a domain controller and/or other server responsible for a directory of broadcast domain features, any combinations thereof, or even other approaches**. Thus, although a gateway device may be referred to as a matter of convenience in connection with a broadcast domain, for example, it is to be understood, of course, that a gateway device is provided as merely one illustration of a network device, such as a network device with capability to perform operations, as described, for example, such as, discovery, reflection, communication with a tunnel server, operating as a tunnel server, operating as a controller, etc. Likewise, a network device may be implemented virtually (e.g., logically) or non-virtually (e.g., physically). Furthermore, in this context, without human intervention indicates that processes may be executed without human intelligence being on hand or otherwise generally available to make appropriate adaptations or changes, such

as, if unanticipated events take place, for example. Throughout this specification, unless otherwise stated, it is intended that a process or processes be interpreted as being executed without human intervention. Thus, one or more processes may execute satisfactorily to accomplish a particular result, without human intelligence, interaction and/or direction, for example. Thus, in a sense, such processes at least may be said to be performed automatically. Typically, although not necessarily, this may include one or more software implemented applications.

EX-1004 14:33-64; EX-1003 ¶109.

A POSITA understood that the discovery and querying of the domain controller and/or directory server—described in Hankins as types of services provided by the network devices—are domain name system lookups. EX-1003 ¶110.

To the extent that PO argues that Hankins does not use the term domain name system lookup, a POSITA understood that domain name service involves querying DNS servers to lookup various records including IP addresses related to domain names. Thus, a POSITA would be motivated to modify the teachings of Hankins to include a domain name system lookup to locate the second device as taught by Munger. Munger discloses a plurality of computer nodes that communicate using seemingly random Internet Protocol source and destination addresses. Packets matching criteria are accepted for further processing, while

those that do not are rejected. Munger discloses a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry. EX-1005 Abstract; EX-1003 ¶111.

Munger discloses a secure mechanism for communicating over the Internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), and uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages (“packets” or “datagrams”). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be the next-hop TARP router as well as the final destination. EX-1005 2:67-3:18; EX-1003 ¶112.

Munger discusses a client computer [*first device*] performs a DNS lookup, e.g., by sending a DNS lookup request to locate a target computer [*second device*]:

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

EX-1005 47:20-33; EX-1003 ¶113.

Munger further teaches a DNS server that “provide[s] a look-up function that returns the IP address of a requested computer or host.” EX-1005 37:22-24; EX-1003 ¶114.

Therefore, it would have been obvious to a POSITA to modify the teachings of Hankins to include in Hankins’ gateway or tunnel server, DNS request functionality as taught by Munger. A POSITA would have been motivated to combine the teachings of Munger and Hankins because:

- 1) It would allow the network device, e.g., gateway or tunnel server, to return an IP address of the target network device outside the domain;
- 2) It would advantageously allow addressing to a target network device [*second device*] located in a separate domain such that IP packets destined for the target network device may be so routed;
- 3) The modification would beneficially reduce the need for another network device to obtain and transmit the DNS information. EX-1003 ¶115.

In addition such a modification would be merely:

- 4) A software implemented solution to include the DNS functionality in a network device that is expressly contemplated by Hankins. EX-1004 14:33-64.
- 5) Choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success (“obvious to try”)--in Hankins, there are only of finite number of network elements which could be selected to perform the well-

known function of DNS look up. Therefore it would have been obvious to select the one of the network devices of Hankins (gateway or tunnel server) to provide the DNS lookup. A POSITA understood that the selection of the gateway or tunnel servers to provide this service would have produced predictable results. EX-1003 ¶116.

A POSITA would also be confident of the success of the combination because the proposed combination would not result in rearrangement of the network devices, network topology, nor a deviation from their common and intended operation/uses, and instead could be implemented in software, a well understood and predictable endeavor. EX-1003 ¶117.

Claim 4

[4] The network system according to claim 1, wherein at least one of the plurality of intermediate access point servers is configured to cache content.

Hankins discloses the tunnel servers [*intermediate access point servers*] may be configured to cache content:

In one embodiment, tunnel server two 370, may store network communications. Network device 322 may comprise a file server, for example. A device, such as network device 312, may request file services from file server 322 via tunnel server two 370. Network device 312 may receive requested services. Subsequently, network device 332 may request similar file services from file server 322 via tunnel 55 server two 370. Tunnel server two 370, having stored

previous requests for file service, for example, may respond by providing a requested file service, without necessarily communicating a request to file server 322. **A tunnel server may, for example, in an embodiment, potentially provide a faster response by storing previous service requests, referred to here as caching the previous service requests.**

EX-1004 27:49-62; EX-1003 ¶118.

In an embodiment, a tunnel server may, for example, store one or more service requests, such as in local memory. In an embodiment, if multiple devices, such as a network device, request similar services, a tunnel server may provide service, or a response to a service request to a requesting device perhaps without forwarding the service request to a device able to initiate service, for example; however, this may vary at least in part on particulars of a situation and/or an embodiment,

EX-1004 27:9-27; EX-1003 ¶118.

Claims 5, 6 and 7

[5] The network system according to claim 1, wherein at least one of the first device, the second device, or the plurality of intermediate access point servers is configured to perform smart routing.

[6] The network system according to claim 5, wherein the smart routing is based on at least one of best bandwidth, lowest latency, fewest hops, or no packet loss.

[7] The network system according to claim 5, wherein smart routing is based on at least one of real-time statistics or historical statistics.

Hankins describes the plurality of tunnel servers and gateway devices are configured to route based upon routing decisions from the controller [*configured to perform smart routing*] that are based upon network data [*information*] including at least available bandwidth and latency [*best bandwidth, lowest latency, real time statistics*]:

Likewise, gateway devices may optionally communicate with other gateway devices, such as via tunnel server one or tunnel server two, for example, depending at least in part on a host of possible factors, such as, geography, latency, utilization, bandwidth (e.g., throughput), efficiency, cost, etc. Furthermore, via a controller, such as 350, a private network may be reconfigured without human intervention, for example, to improve performance and/or reduce cost. For example, if available bandwidth decreases, if latency increases, and/or if network utilization increases, controller 350 may provision additional tunnel servers or may provision tunnel servers in a manner to improve performance and/or reduce cost without human intervention.

Examples of possible monitoring and/or measurement of network performance and/or cost-related parameter were previously discussed.

EX-1004 25:40-55; EX-1003 ¶119.

Thus, Hankins discloses using automated processes to adapt to changing conditions, *e.g.*, if bandwidth decreases, if latency increases,

and/or if network utilization increases, which use real-time statistics to configure and reconfigure the system. EX-1003 ¶120.

Hankins further discloses that the configuration and reconfiguration includes selecting tunnel servers in close proximity to endpoint to increase the quality of the connection:

A path or channel for communications may potentially be enhanced by controller 350 provisioning an additional tunnel server located more physically proximate to logical broadcast domain C 330 and logical broadcast domain D 340, for example.

EX-1004 25:14-19; EX-1003 ¶121.

Hankins disclosure is consistent with the disclosure of the '505 Patent that smart routing uses algorithmic analysis and other methodologies to adapt to changing conditions and learning over time to configure and reconfigure the system, and by selecting encrypted tunnels between the EPD and access point servers in close proximity to the EPD to improve the quality of the connection.

EX-1001 3:17-30; EX-1003 ¶122.

A POSITA understood that the factors upon which the tunneling servers were provisioned described in Hankins including geography, latency, utilization, bandwidth (e.g., throughput), efficiency, cost, etc. are real time or historical statistics. Additionally a POSITA understood that selection based upon best

bandwidth or latency is a selection based on the available bandwidth or lowest latency respectively. EX-1003 ¶123

Claims 8 and 10

[8] The network system according to claim 1, wherein at least one of the first device, the second device, or the plurality of intermediate access point servers is configured to perform firewall services.

[10] The network system according to claim 8, wherein a first intermediate access point server among the plurality of intermediate access point servers provides firewall services between the first device and other intermediate access point servers among the plurality of intermediate access point servers or the second device.

Hankins discloses the tunnel servers [*a first intermediate access point server*] perform/provide firewall services with respect to the transiting signal packets between the gateway device 311 [*first device*] and gateway device 321 [*second device*]:

At block 424, one or more tunnel servers may receive signal packets and may initiate services. Services may include, for example, a private network policy and inspection process, which may include, as examples, virus scanning, filtering (for example, URL filtering), deep packet inspection, **a firewall**, and others, in connection with processing of the received signal packets.

EX-1004 29:1-8; EX-1003 ¶124.

Claim 9

[9] The network system according to claim 8, wherein the first device provides firewall services between the first device and the plurality of intermediate access point servers.

Hankins discloses the gateway devices [*first device*] communicates with the tunnel server [*intermediate access point server*] and may provide firewall services between the gateway device and the tunnel server:

A possible feature for one or more private networks may include a capability implement a private network policy and inspection process. For example, a unified networking policy may be implemented, despite potentially being physically or logically separate networks and/or physically or logically separate sub-networks, for example. Likewise, private network policy and inspection process may include selected networks and/or sub-networks employing selected policies or selected networks and/or sub-networks employing a unified policy. A selected or a unified **networking policy may, for example, include** particulars regarding implementing at least one of the following processes: virus scanning, authentication, filtering (for example, URL filtering), deep packet inspection, encryption, a **firewall**, or any combinations thereof.

EX-1004 18:46-60; Annotated FIG. 2; EX-1003 ¶125.

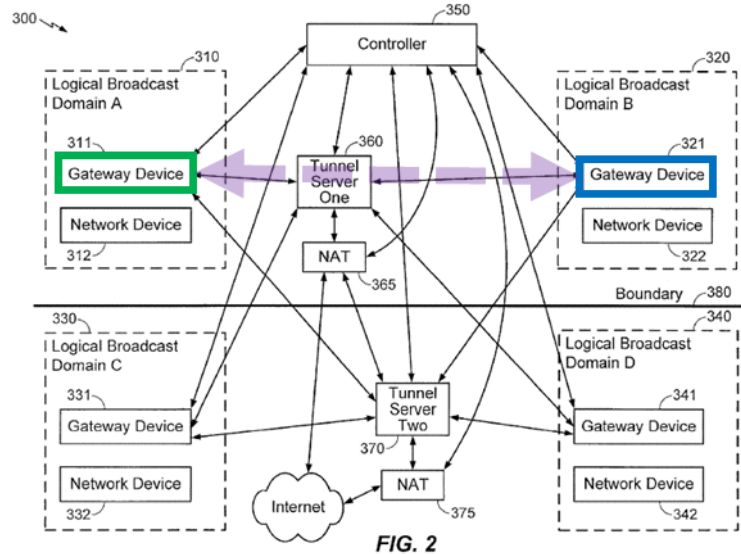
Hankins discloses the gateway devices, as well as other network devices implement network policy, and therefore a POSITA understood that the gateway

provides firewall services between the gateway and the tunnel server. EX-1004 14:33-64, 29:1-8; EX-1003 ¶126. Furthermore, implementing firewall services at a gateway or other network device was well-known in the art. EX-1003 ¶127.

Claim 11

[11.0] A method comprising:

Hankins discloses a method for communicating packets from one gateway/network device to another:



EX-1004 FIG. 2; EX-1003 ¶128.

[11.1] establishing, by one or more computer processors, a plurality of end-to-end tunnels between a first device and a second device, the plurality of end-to-end tunnels being configured to carry network traffic via a plurality of intermediate access point servers;

With reference to Annotated FIG 2, Hankins discloses establishing by gateway devices, controllers, and tunnel servers [*computer processors*], a plurality of paths/channels [*end-to-end tunnels*] between a gateway device in a first domain (**green**) [*first device*] and a gateway device in a second domain (**blue**) [*second device*], where the paths/channels carry network traffic via a plurality of tunnel servers (**red**) [*intermediate access point servers*]:

As an example, gateway device 311 may transmit signal packets to gateway device 321. Gateway device 311 may transmit signal packets via tunnel server one 360 since tunnel server one 360 is more proximate to both gateway device 311 and gateway device 321 in this example. In another embodiment, gateway device 311 may transmit signal packets via tunnel server two 370...

EX-1004, 25:56-62; EX-1003 ¶129.

Hankins further discloses that the signal packets may be encapsulated, which allows the gateway devices via the tunnel servers to be connected/linked across domains via the paths or channels:

Thus, for example, if a virtual broadcast domain provides a signal packet A to a tunnel server, it may be encapsulated.... [A] tunnel server may likewise remove encapsulation (e.g., referred to as termination) to determine where to forward a signal packet and re-encapsulate it for forwarding.

EX-1004 13:8-14; EX-1003 ¶130.

A path or channel for communications may potentially be enhanced by controller 350 provisioning an additional tunnel server located more physically proximate to logical broadcast domain C 330 and logical broadcast domain D 340, for example. Controller 350 may provision tunnel server two 370.

EX-1004 25:15-20; EX-1003 ¶130.

A tunnel server may forward traffic (e.g., signal packet transmissions) between gateway devices, for example, such as for communications between different logical broadcast domains

EX-1004 12:63-64; EX-1003 ¶130.

The term tunnel server refers to a mechanism or technique capable of being implemented in a network, such as in software, firmware, hardware or any combination thereof (other than software per se, since software is executed, of course, typically on one or more computing devices), that includes a capability to link logical broadcast domains, such as via encapsulation of signal packets, as previously described,

EX-1004 13:46-54; EX-1003 ¶130.

[11.2] *receiving, by the one or more computer processors, information from at least one of the plurality of intermediate access point servers; and selecting, by the one or more computer processors, one of the plurality of end-to-end tunnels for communication*

between the first and second devices based on the information.

Hankins discloses the controller (**gold**) [*one or more computer processors*] receives information regarding the network and provisions [*selects*] tunnel servers along with one of the paths or channels [*end-to-end tunnels*] for communications between the gateway devices [*first and second devices*] based upon the received information, for the same reasons as discussed with respect to limitation [1.4]. EX-1003 ¶131.

Claim 12

The method according to claim 11, further comprising configuring, by the one or more computer processors, at least one of the first device or the plurality of intermediate access point servers to perform a domain name system lookup to locate the second device.

Hankins discloses that each of the network devices inclusive of gateways [*first and second devices*] and tunnel servers [*intermediate access point servers*] are configured to provide services, including domain name system lookups for other network devices such as gateway 321 [*second device*] for the same reasons as discussed with respect to Claim 2. EX-1003 ¶132.

Claim 14

[14.0] *A system comprising:*

Hankins discloses a private network [*system*] that communicates packets from one network device to another:

Furthermore, the at least one private network communicates selected signal packets from at least one network device in one of at least two separate logical broadcast domains transmitted to at least one network device in another of at least two separate logical broadcast domains as if the logical broadcast domains are not separate. The selected signal packets are transmitted between the network devices of the at least two separate logical broadcast domains via a tunnel server.

EX-1004 Abstract; EX-1003 ¶ 133.

[14.1] *a memory storing instructions; and*

Hankins discloses network devices and computing devices, and discloses that such devices include a memory (gold) that stores instructions:

FIG. 5 is an illustration of an embodiment of a computing platform 1150 that may be employed in a client-server type interaction, such as described infra. in connection with rendering a GUI via a 20 device, such as a network device and/or a computing device.

EX-1004, 33:17-21; EX-1003 ¶ 134.

Memory 1170 may be representative of any storage mechanism. Memory 1170 may comprise, for example, primary memory 1174 and secondary memory 1176, additional memory circuits, mechanisms, or combinations thereof may be used. Memory 370 may comprise, for example, random access memory, read only memory, or one or more data storage devices or systems, such as, for example, a disk drive, an optical disc drive, a tape drive, a solid-state memory drive, just to name a few examples. Memory 1170 may be utilized to store a

program. Memory 1170 may also comprise a memory controller for accessing computer readable-medium 1175 that may carry and/or make accessible content, code, and/or instructions, for example, executable by processor 1160 or some other controller or processor capable of executing instructions, for example.

EX-1004, 33:55-34:4; EX-1003 ¶ 134.

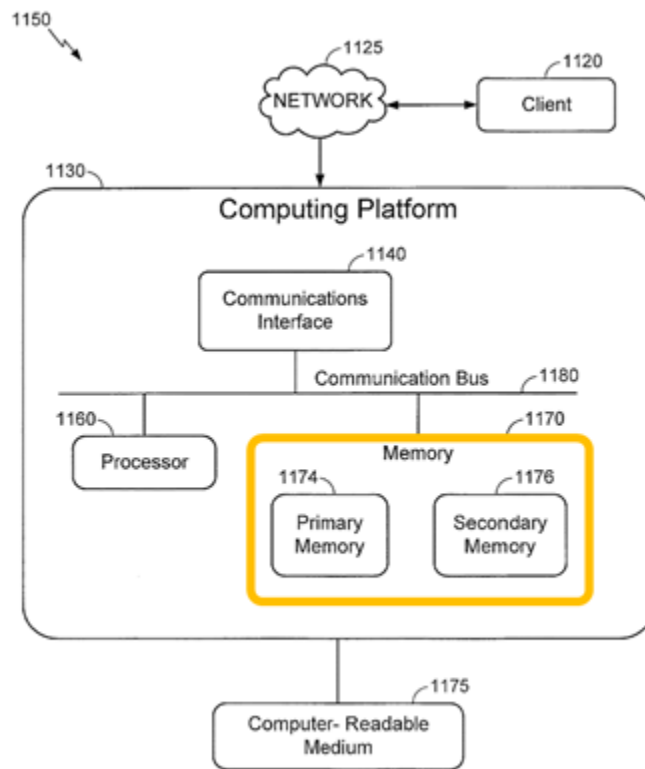


FIG. 5

EX-1004 FIG. 5; EX-1003 ¶ 134

[14.2]. one or more processors coupled to the memory, the one or more processors being configured to execute the instructions, the instructions causing the one or more processors to perform operations comprising:

Hankins discloses network devices and computing devices (e.g. controller, gateways, tunnel servers) [*one or more processors*] configured to execute instructions causing the network devices and/or computing devices to perform operations:

A system comprising: a computing device including at least one processor, at least one memory, and at least one display; the computing device to execute on the at least one processor computer instructions that are stored on the at least one memory;

EX-1004 41:57-61(Claim 54); EX-1003 ¶135.

A network device may comprise, as non-limiting examples, a router, gateway, hub, switch, host, mobile device, server, client, NAT device, the like, or any combinations thereof.

EX-1004 8:15-19; EX-1003 ¶135.

Furthermore, in another embodiment, a tunnel server may comprise a network device physically, logically, virtually or non-virtually separate from a controller.

EX-1004, 13:64-67

Hankins discloses the network devices and computing devices (**pink**) [*one or more processors*] are configured to execute instructions causing the network devices and/or computing devices to perform operations:

A computing and/or network device may also include or execute a software application to perform a variety of possible tasks,

EX-1004 36:4-6; EX-1003 ¶136.

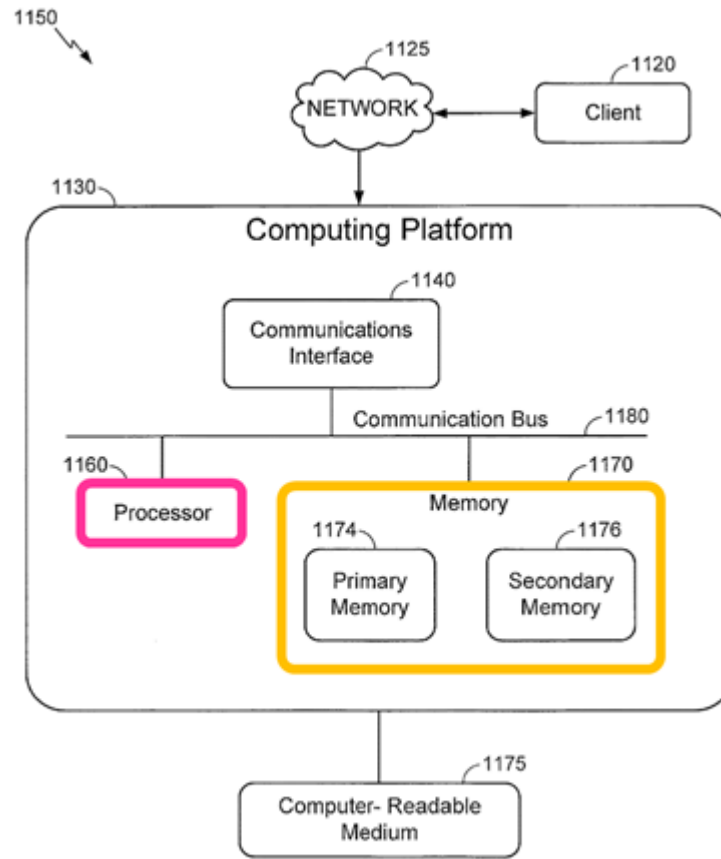


FIG. 5

EX-1004 FIG. 5; EX-1003 ¶136.

Hankins discloses the controller, tunnel servers and gateways may be implemented by instructions carried out by a device and/or by a software application executing instructions. EX-1004 8:12-19, 13:47-51, 16:47-50; EX-1003 ¶137.

[14.3] *establishing a plurality of end-to-end tunnels between a first device and a second device, the plurality of end-to-end tunnels being configured to carry network traffic via a plurality of intermediate access point servers;*

Hankins discloses a first device 311 (**green**) and a second device 321 (**blue**), a plurality of access point servers including tunnel server one (**red**) and tunnel server two (**red**) [*intermediate access point servers*] that each form a plurality of end-to-end tunnels for the same reasons as discussed with respect to limitation [1.3]. EX-1003 ¶138.

[14.4] *receiving information from at least one of the intermediate access point servers; and selecting one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information.*

Hankins discloses a controller 350 (**gold**) [*one or more processors*] that receives information regarding the network and provisions tunnel servers along with one of the end-to-end tunnels for communications between the gateway devices [*first and second devices*] based upon the received information for the same reasons as discussed with respect to limitation [1.4]. EX-1003 ¶139.

Claims 15, 16 and 17

[15] *The system according to claim 14, wherein the operations further comprise configuring at least one of the first device, the second device, or the plurality of*

intermediate access point servers to perform smart routing.

[16] The system according to claim 15, wherein the smart routing is based on at least one of best bandwidth, lowest latency, fewest hops, or no packet loss.

[17] The system according to claim 15, wherein the smart routing is based on at least one of real-time statistics or historical statistics.

Hankins describes the plurality of tunnel servers and gateway devices are configured to route based upon routing decisions from the controller [*configured to perform smart routing*] that are based upon network data [*information*] including at least available bandwidth, and latency [*best bandwidth, lowest latency, real time statistics*] for the same reasons as discussed with respect to Claims 5, 6 and 7. EX-1004 25:14-19,40-55; EX-1003 ¶139.

Claims 18 and 20

[18] The system according to claim 14, wherein the operations further comprise configuring at least one of the first device, the second device, or the plurality of intermediate access point servers is configured to perform firewall services.

[20] The system according to claim 18, wherein a first intermediate access point server among the plurality of intermediate access point servers provides firewall services between the first device and other intermediate access point servers among the plurality of intermediate access point servers or the second device.

Hankins discloses the tunnels servers [*a first intermediate access point server*] perform/provides firewall services with respect to the transiting signal packets between the gateway device 311 [*first device*] and gateway device 321 [*second device*] for the same reasons as discussed with respect to Claims 8 and 10. EX-1004 29:1-8; EX-1003 ¶140.

Claim 19

The system according to claim 18, wherein the first device provides firewall services between the first device and the plurality of intermediate access point servers.

Hankins discloses the Gateway devices [*first device*] may provide firewall services between the Gateway device and the tunnel server [*intermediate access point server*] for the same reasons as discussed with respect to Claim 9. EX-1004 14:33-64, 18:46-60, 29:1-8; EX-1003 ¶141.

B. Ground 2: Claims 3 and 13 are unpatentable over Hankins, alone, or in view of Munger, or further in view of Treuhaft,

1. The Treuhaft Reference

Treuhaft discloses systems and methods for processing domain name system requests (DNS requests) in a network. EX-1009 Abstract; EX-1003 ¶142.

Treuhaft describes network resources such as those available via the Internet are accessed according to Internet Protocol (IP) addresses. IP addresses are represented numerically, traditionally as a quartet of values having the form

111.111.111.111. From the early inception of network computing, familiar alphanumeric name-based addressing has been used to allow users to more easily locate and remember the addresses for resources. For example, domain names are assigned to computing servers and clients. The domain name system facilitates the translation between IP addresses and domain names by maintaining accessible records that associate one or more domain names with one or more IP addresses. EX-1009 [0004]; EX-1003 ¶143.

Treuhaft describes when a nameserver (network server) receives a DNS request, it first checks a local cache to attempt to resolve the request. The DNS nameserver maintains the local cache with domain name records that have already been resolved to improve performance in responding to subsequent DNS requests. If the nameserver is maintaining the requested domain name in the local cache, it will issue a DNS response to the client with the domain name record including the IP address corresponding to the request. EX-1009 [0006]; EX-1003 ¶144.

If the nameserver does not have an entry for the requested domain name, it will launch recursive processing to obtain it. EX-1009 [0007]; EX-1003 ¶145.

2. Detailed Application of Hankins, Munger and Treuhaft to Claims 3 and 13

Claims 3 and 13

[3] The network system according to claim 1, wherein at least one of the first device or the plurality of

intermediate access point servers is configured to perform a domain name system lookup from a cache to locate the second device.

[13] The method according to claim 11, further comprising configuring, by the one or more computer processors, at least one of the first device or the plurality of intermediate access point servers to perform a domain name system lookup from a cache to locate the second device.

A described above with respect to Claim 2, Hankins alone, or in view of Munger, discloses performing DNS lookup services in the network devices (e.g. gateways, tunnel servers etc.) to locate a device such as gateway 321 [*second device*]. See VI.A.2. Claim 2 above. In addition, Hankins discloses the use of caching for prior service requests by the tunnel servers:

[T]he tunnel server may, for example, in an embodiment potentially provide a faster response by storing previous service requests, referred to here as **caching the previous service requests**.

EX-1004 27:56-62; EX-1003 ¶146.

To the extent that PO argues Hankins, alone, or in view of Munger does not explicitly disclose the DNS service is performed from a cache, Treuhaft discloses this feature. Treuhaft discloses performing a domain name system lookup from a cache. EX-1009 [0006,0007]; EX-1003 ¶147.

Treuhaf discloses the server receives a DNS request and first checks its cache for the requested information, otherwise it subsequently obtains the information from other network devices:

Consider an example DNS request 150 from client 102 to nameserver 112 for the domain name information of `www.opendns.com`. The ISP DNS nameserver first checks a local cache to attempt to resolve the request. The ISP DNS nameserver maintains the local cache with domain name records that have already been resolved to improve performance in responding to subsequent DNS requests. If nameserver 112 is maintaining the requested domain name in the local cache, it will issue a DNS response 152 to the client with the domain name record including the IP address of “`www.opendns.com`.”

EX-1009 [0006]; EX-1003 ¶148.

If the ISP DNS nameserver 112 does not have an entry for the requested domain name, it will launch recursive processing using authoritative DNS nameservers 120 and/or root DNS nameservers 130. An authoritative nameserver maintains an authoritative or master list for a Zone which is a group of computing devices. Recursive DNS nameservers obtain domain name information such as the IP address of a requested resource from authoritative nameservers. The root DNS nameservers are also authoritative DNS nameservers. They are called root DNS nameservers because they contain the authoritative domain name information for a set of top level domains (TLDs) in the so-called root Zone. For example the root DNS nameservers contain the IP addresses for finding domain name information for lower level

domains in the top level domains. The top level domains include the generic top-level domains (gTLD) of .com, .org, .net, etc.

EX-1009 [0007]; EX-1003 ¶148.

Treuhaft specifically discloses the use of a “local cache with domain name records that have already been resolved to improve performance in responding to subsequent DNS requests.” EX-1009 [0006]; EX-1003 ¶149.

Therefore, it would have been obvious to a POSITA to modify the teachings of Hankins alone, or in view with Munger, and include use of a cache into Hankins network devices, (e.g., gateway or tunnel server) as taught by Treuhaft. A POSITA would have been motivated to combine the teachings of Treuhaft and Hankins, or Hankins in view of Munger because:

1) It would allow the network device to return an IP address of the target network device outside the domain, without an additional query when the results of a recent query results is within the cache;

2) It would advantageously improve the performance of the DNS look up function, specifically increasing the speed of response;

3) The modification would beneficially reduce the need for another network device to obtain and transmit the DNS information. EX-1003 ¶150.

In addition such a modification would be merely the use of a known technique (e.g., local caches to store previously retrieved DNS information) to

improve similar devices (e.g., the network devices of Hankins receiving DNS service requests) in the same way (e.g., to improve response time and minimize network traffic). EX-1003 ¶151.

A POSITA understood that implementation of a cache in performing DNS services in Hankins network devices (e.g., the gateway or tunnel servers) would have produced predictable results. EX-1003 ¶152.

A POSITA would also be confident of the success of the combinations because the proposed combination would not result in rearrangement of the network devices, network topology, nor a deviation from their common and intended operation/uses. Allocating tasks among the various network devices was a well-understood and predictable endeavor. EX-1003 ¶153.

VII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION

A. The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)

The Board has discretion to deny institution under 35 U.S.C. § 314(a).

Related to the Director's June 2022 interim guidance regarding application of the *Fintiv* factors², (1) the Petition is particularly strong in the underlying merits, and

² Interim Procedure For Discretionary Denials In AIA Post Grant Proceedings With Parallel District Court Litigation, PTO Director's Memorandum (June 21, 2022).

(2) the Petitioner adopts the identical stipulation from *Sotera*, namely, that if the IPR is instituted, Petitioner will not pursue in the Related Litigation any ground raised or that could have been reasonably raised in an IPR for the challenged patent. Thus, under the Interim Guidance, the Board should not deny institution.

Nevertheless, the Board's decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (Dec. 1, 2020) instructs that a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed.

Under factor 2, trial date has been set for August 10th-14, 2026. A Final Written Decision is expected in the present matter in August 2025, 12 months before trial in the Related Litigation. Thus, this factor weighs against discretionary denial.

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. The parties have not exchanged proposed claim terms or constructions, and will not complete claim construction briefing until October 2024. The Markman hearing is not until December 2024. Fact discovery is not set to close until September 2025, and expert discovery is not set to close until February 5, 2026.; *See PEAG LLC v. Varta Microbattery GMBH*, IPR2020-01214, Paper 8 at 17 (Jan. 6, 2021) (finding that since no claim construction hearing had yet been held and discovery was not completed, the little

investment in the parallel proceeding weighed against discretionary denial). Thus, this factor weighs against discretionary denial.

Under factor 4, in addition to the *Sotera* stipulation that Petitioner issued to PO, PO has only identified in the Complaint a subset of the claims that are being challenged in the present Petition. Thus, it is unlikely the district court will be addressing the validity of all of the claims challenged by this Petition.

Under factor 5, Petitioner is a defendant in the Related Litigation. Nothing within *Fintiv* suggests that the same party between the proceedings weighs in favor of discretionary denial. *See HP Inc. v. Slingshot Printing LLC*, IPR2020-01084, Paper 13 at 9 (having the “same parties as parallel proceeding” makes factor 5 “neutral”)).

Under factor 6, other circumstances weigh in favor of institution. Here, the merits of the Petition are particularly strong. For example, Hankins is a parallel disclosure to the '505 Patent, meaning that it is directed at the same problem and proposes the same solution as the '505 Patent, and discloses identical architecture and the identical concepts disclosed in the '505 Patent, but uses some different words, thus demonstrating that the Petition is particularly strong in the underlying merits. The evidence presented, if unrebutted in trial, would plainly lead to a

conclusion that one or more claims are unpatentable by a preponderance of the evidence.

When viewed holistically, the timing of the present Petition is reasonable, there has been relatively limited investment in the Related Litigation, and there is minimal overlap between the present IPR and the Related Litigation. Further, coupling these *Fintiv* considerations with compelling evidence of unpatentability presented in the Petition, the efficiency and integrity of the IPR process is best served by instituting review.

VIII. Mandatory Notices Under 37 C.F.R. §42.8

A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))

The real party-in-interest in this Petition is CISCO SYSTEMS, INC..

B. Related Matters (37 C.F.R. § 42.8(b)(2))

1. Judicial Matters

As of the filing date of this Petition and to the best knowledge of Petitioner, the '505 Patent is involved in the following litigations:

UMBRA Technologies Ltd. (UK) et al v. Cisco Systems, Inc., Case No. 1:23-cv-00903-DII (W.D. Tex.) (filed Aug. 2, 2023) (ongoing)

UMBRA Technologies Ltd. (UK) et al v. VMware, Inc., Case No. 1:23-cv-00904-DII (W.D. Tex.) (filed Aug. 2, 2023) (ongoing).

2. Administrative Matters:

As of the filing date of this Petition and to the best knowledge of Petitioner, the '505 Patent was not subject to any previous *inter partes* reviews.

3. Related Patents

See Exhibit. EX-1010

C. Lead/Back-up Counsel (37 C.F.R. § 42.8(b)(3)):

Lead Counsel:

Patrick D. McPherson, USPTO Reg. No. 46,255
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East,
Washington, D.C. 20001
P: (202) 776-5214; F: (202) 776-7801; PDMcPherson@duanemorris.com

Back-Up Counsel: Patrick C. Muldoon, USPTO Reg. No. 47,343
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East,
Washington, D.C. 20001
P: (202) 776-7840; F: (202) 776-7801; PCMuldoon@duanemorris.com
Joseph English, USPTO Reg. No. 42,514
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East,
Washington, D.C. 20001
P: (202) 776-5228; F: (202) 776-7801; DJEnglish@duanemorris.com

D. Notice of Service Information (37 C.F.R. § 42.8(b)(4)):

Please direct all correspondence to lead and back-up counsel at the above addresses. Petitioner consents to electronic service at the email addresses above.

IX. CONCLUSION

For the reasons set forth above, Petitioner has established a reasonable likelihood of prevailing with respect to all Challenged Claims of the '505 Patent and requests the Board institute *inter partes* review and then cancel all claims as unpatentable.

Respectfully submitted,

DUANE MORRIS LLP

BY: /Patrick D. McPherson/
Patrick D. McPherson
USPTO Reg. No. 46,255
Duane Morris LLP
901 New York Ave NW, Suite 700
East
Washington, D.C. 20001

Dated: February 26, 2024

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§ 42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on February 26, 2024, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent No. 10,630,505 and all supporting exhibits were served via Federal Express, postage prepaid, to Umbra Technologies LTD by serving the correspondence address of record for the '505 Patent:

Gardella Grace P.A.
80 M Street SE, 1st Floor
Washington, DC 20003
UNITED STATES

/Patrick D. McPherson/
Patrick D. McPherson, Reg. No. 46,255
901 New York Ave NW, Suite 700 East
Washington, D.C. 20001
P: (202) 776-7800
F: (202) 776-7801
PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this document complies with the type-volume limitations. This document contains 12,447 words as calculated by the “Word Count” feature of Microsoft Word 2010, the word processing program used to create it.

Dated: February 26, 2024

By: Patrick D. McPherson

Patrick D. McPherson

Reg. No. 46,255

Duane Morris LLP

901 New York Ave NW,

Suite 700 East

Washington, D.C.

P: (202) 776-7800

F: (202) 776-7801

PDMcPherson@duanemorris.com