

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.
Petitioner,

v.

OPTIMNET LLC,
Patent Owner,

U.S. Patent No. 8,780,887

Issue Date: July 15, 2014

Title: METHOD OF NETWORK-BASED COMMUNICATION IN VIRTUAL
NETWORK ENVIRONMENT

Inter Partes Review No.: IPR2026-00320

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 8,780,887
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. GROUND FOR STANDING 37 C.F.R. § 42.104(A)	2
IV. REASONS FOR THE REQUESTED RELIEF	2
A. Overview of the '887 Patent.....	2
B. Prosecution History of the '887 Patent	5
C. Priority Date of the Challenged Claims	6
D. Claim Construction	6
E. Level of Ordinary Skill in the Art	6
F. State of the Art	7
V. IDENTIFICATION OF HOW CLAIMS ARE UNPATENTABLE	13
A. Ground 1: Claims 1-10.....	13
1. The Pankratov Reference	13
2. Detailed Application of Pankratov to the Challenged Claims	15
Claim 1	15
Claim 2.....	24
Claim 3	26
Claim 4.....	29
Claim 5	29
Claim 6.....	32
Claim 7	35
Claim 8.....	37
Claim 9	39

Claim 10.....	42
VI. MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	42
A. Real Party-in-Interest Under 37 C.F.R. §42.8(b)(1)	42
B. Related Matters Under 37 C.F.R. § 42.8(b)(2)	43
1. Judicial Matters.....	43
2. Administrative Matters	43
3. Related Patents	43
C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	43
D. Service Information 37 C.F.R. §42.8(b)(4).....	44
E. Payment of Fees – 37 C.F.R. §42.103.....	44
VII. CONCLUSION	44

TABLE OF AUTHORITIES

Federal Statutes

35 U.S.C. § 102(b)	13
35 U.S.C. § 103	1, 13
35 U.S.C. § 112	5-6

Regulations

37 C.F.R. § 42.8	43
37 C.F.R. § 42.8(b)(1)	43
37 C.F.R. § 42.8(b)(2)	43
37 C.F.R. § 42.8(b)(3)	44
37 C.F.R. § 42.8(b)(4)	44
37 C.F.R. § 42.103	44
37 C.F.R. § 42.104(A)	2

PETITIONER'S EXHIBIT LIST

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 8,780,887 (“the ’887 Patent”)
1002	Prosecution History of the ’887 Patent (“File History”)
1003	Declaration of Petitioner’s Expert
1004	U.S. Patent Publication No. 2007/0157303 to Pankratov (“Pankratov”)
1005	Brian Ford et al., <i>Peer-to-Peer Communication Across Network Address Translators</i> , ATEC '05: Proceedings of the USENIX Annual Technical Conference, Apr. 14, 2005.
1006	Ex. C of OptimNet’s Infringement Contentions Against Petitioner for the ’887 Patent in <i>OptimNet LLC v. Cisco Systems, INC</i> , No. 2:25-cv-00935-JRG (E.D. Tex.)

I. INTRODUCTION

Cisco Systems, Inc. (“Petitioner”) hereby petitions for an *inter partes* review (IPR) of U.S. Patent No. 8,780,887 (“the ’887 Patent”, EX-1001). Petitioner respectfully submits that Claims 1-10, (the “Challenged Claims”) of the ’887 Patent are unpatentable under 35 U.S.C. § in view of following ground:

Grounds	Claims	Basis	References
Ground 1	1-10	35 U.S.C. §103	Pankratov

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.

II. OVERVIEW

The ’887 Patent is directed to network-based communications in a virtual network environment where communication nodes are behind a network address translation (NAT) device. Using a known hole-punching mechanism, the ’887 Patent described using a tunnel mapping controller to establish a tunnel for direct communications between the nodes.

However, it was well-known to use hole-punching to establish direct communications using tunnels between communication nodes that were behind NAT devices. The Pankratov reference discloses using a hole-punching

mechanism, and a meditation server as a tunnel mapping controller to establish a tunnel to establish direct communications between the nodes. Thus, the Challenged Claim are unpatentable over the Pankratov reference.

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

Petitioner certifies that the '887 Patent is available for IPR.

IV. REASONS FOR THE REQUESTED RELIEF

As explained in §§II and IV-V of this Petition and in the attached Declaration of Petitioner's Expert, EX-1003, the subject matter claimed in the '887 Patent was obvious over the prior art to a person of ordinary skill in the art ("POSITA") at the time of the purported invention.

A. Overview of the '887 Patent

The '887 Patent is directed to network-based communications in a virtual network environment. One problem identified in the '887 Patent is that when virtual nodes are connected to the internet through a network address translation (NAT) device or firewall, there are problems with establishing direct communication between the nodes because the internal IP addresses are not known. EX-1001 3:19-24. The '887 Patent's proposed solution was to utilize a tunnel mapping controller to establish tunnels between the nodes to allow direct communication. EX-1001 6:8-14.

In one embodiment, virtual tunnel routers (TRs) operate as network components which form one or more virtual networks. EX-1001 5:39-40. A

tunnel mapping controller serves to process and control tunneling between virtual TRs. The tunnel mapping controller establishes an IP tunnel in conjunction with each of the virtual TRs and connects each virtual IP prefix to the established tunnel, thus enabling direct communication between virtual networks. EX-1001 6:8-14.

The tunnel mapping controller includes a virtual network prefix information table. EX-1001 6:15-16. “Virtual network prefix information is addresses assigned to terminals or devices connected to respective virtual networks. For example, if a virtual network has a prefix and length of 1.1.1.0/24, each terminal connected to the virtual network is assigned one IP in the range from 1.1.1.1 to 1.1.1.255, which is virtual network prefix information.” EX-1001 6:48-53. The network prefix information is generated by the tunnel mapping controller or predetermined by an administrator, provided to the virtual TRs, and then stored in a database. EX-1001 6:53-61. When the virtual TRs request virtual network prefix information after registering themselves, the tunnel mapping controller allocates and forwards virtual network prefixes to the virtual TRs. EX-1001 6:16-20.

In the process of registering the virtual TRs in the tunnel mapping controller, a NAT traversal function or a Session Traversal Utilities for NAT (STUN) procedure is performed together to learn the incorporation of an NAT/firewall. The

information learned through this procedure is used as information such as mapped IP/port across the NAT and network connection type or network operation mode to be used later in a virtual TR tunneling process. The NAT traversal function or STUN procedure is a well-known technology referred to as “hole-punching” and the ’887 patent explains that a detailed description thereof was therefore omitted. EX-1001 50-60.

When the TRs are connected to the virtual network, the tunnel mapping controller creates information of a list of virtual TRs for tunneling and reports it to the TRs in order to notify the TRs that the currently registered first virtual TR and second virtual TR are targets to be tunneled for direct communication. The information of a list of virtual TRs for tunneling contains information such as the mapped IP/port, network connection type, and operation mode of a connected network to be used for the hole punching process. When each virtual TR receives the information of a list of virtual TRs for tunneling, a hole punching message for UDP/ TCP Hole Punching is exchanged in order to establish a tunnel with the virtual TR. Then, each virtual TR determines whether the transmission and reception of the hole punching message are successful. If the message transmission and reception are successful, a tunnel establishment message is exchanged. EX-1001 8:1-25.

The '887 Patent issued with ten claims, with Claims 1 and 6 as independent.

Claim 1 is representative:

1. A communication method that provides end-to-end communication in a virtual network environment, the method comprising:

a plurality of virtual tunnel routers comprising a first virtual tunnel router and a second virtual tunnel router receiving a message containing virtual network prefix information from a tunnel mapping controller;

determining whether the first virtual tunnel router has received a hole punching message from the second virtual tunnel router;

if the first virtual tunnel router has received a hole punching message, the first virtual tunnel router establishing a tunnel with the second virtual tunnel router based on the virtual network prefix information; and

the first virtual tunnel router performing direct communication with the second virtual tunnel router will be omitted in the exemplary embodiment of the present invention.

B. Prosecution History of the '887 Patent

The '887 Patent issued from Application Serial No. 13/234,425 filed on September 16, 2011, claiming priority to Korean Patent Application No. 10-2010-0107107 filed October 29, 2010. EX-1001 (21-22). During prosecution the examiner rejected Claim 1 under 35 U.S.C. §112 because the recited term “hole punching message” was unclear and the essential elements for the mechanism for

performing hole punching were omitted. EX-1002 p. 123. In response, the Applicant asserted that hole punching elements and steps associated with it were well-known as demonstrated by a prior art reference cited by the examiner, U.S. Pat. Pub. 2011/008294. EX-1002 p. 145. In response, the examiner withdrew the 35 U.S.C. §112 rejections.

C. Priority Date of the Challenged Claims

The '887 Patent claims priority to October 29, 2010. EX-1001. This Petition assumes that date as the “Priority Date.”

D. 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. EX-1003 ¶¶36-37.

E. Level of Ordinary Skill in the Art

A Person of Ordinary Skill in the Art (“POSITA”) in October 2011 would have been someone knowledgeable and familiar with network based communications including virtual networks. A POSITA would have gained knowledge of these concepts through a mixture of training and work experience, such as by having at least a bachelor’s degree in electrical engineering or computer engineering or science, or related field, and at least two to three years of training or additional work experience in the area of network communications, or a related

field. Additional hands-on and design experience could compensate for less formal education, and vice versa. The knowledge and skill of a POSITA is further reflected in the prior art references themselves, as well as the State of the Art, discussed below. EX-1003 ¶¶39-42.

F. State of the Art

This section describes the state of the art as of the Priority Date. This section, and the expert testimony and documentary evidence cited, provide additional factual support for the general knowledge, common understanding and skill of a POSITA at the Priority Date. This section provides additional factual support and motivation to modify and combine the teachings in the references, and further demonstrates why doing so would involve a reasonable expectation of success. EX-1003 ¶¶43-52.

Network Address Translation (NAT) causes well-known difficulties for peer-to-peer (P2P) communication, since the peers involved may not be reachable at any globally valid IP address. The Internet's original uniform address architecture, in which every node has a globally unique IP address and can communicate directly with every other node, has been replaced with a new de facto Internet address architecture, consisting of a global address realm and many private address realms interconnected by Network Address Translators (NAT). EX-1005 p. 1.

In this address architecture, only nodes in the “main,” global address realm could be easily contacted from anywhere in the network, because only they have unique, globally routable IP addresses. Nodes on private networks could connect to other nodes on the same private network, and they could usually open TCP or UDP connections to “well-known” nodes in the global address realm. NATs on the path allocated temporary public endpoints for outgoing connections, and translated the addresses and port numbers in packets comprising those sessions, while generally blocking all incoming traffic unless otherwise specifically configured. EX-1005 p. 1.

The Internet's new de facto address architecture was suitable for client/server communication in the typical case when the client was on a private network and the server was in the global address realm. The architecture made it difficult for two nodes on different private networks to contact each other directly, however, which was often important to the “peer-to-peer” communication protocols used in applications such as teleconferencing and online gaming. EX-1005 pp. 1-2.

One prior art method of establishing peer-to-peer communication between hosts on different private networks was known as “hole punching.” This technique was widely used in UDP-based and TCP-based applications. Hole punching enabled applications to function within the default security policy of most NATs,

effectively signaling to NATs on the path that peer-to-peer communication sessions were “solicited” and thus should be accepted. EX-1005 p. 2.

UDP hole punching enabled two clients to set up a direct peer-to-peer UDP session with the help of a well-known rendezvous server, even if the clients were both behind NATs. Hole punching assumes that the two clients, A and B, already have active UDP sessions with a rendezvous server S. When a client registered with server S, the server recorded two endpoints for that client: the (Private IP address, UDP port) pair that the client believed itself to be using to talk with S, and the (Public IP address, UDP port) pair that the server observed the client to be using to talk with it. These endpoints were referred to as the client’s private endpoint and the client’s public endpoint, respectively. The server typically obtained the client’s private endpoint from the client itself in a field in the body of the client’s registration message, and obtained the client’s public endpoint from the source IP address and source UDP port fields in the IP and UDP headers of that registration message. EX-1005 p. 3.

Figure 5 illustrates hole punching where clients A and B had private IP addresses behind different NATs.

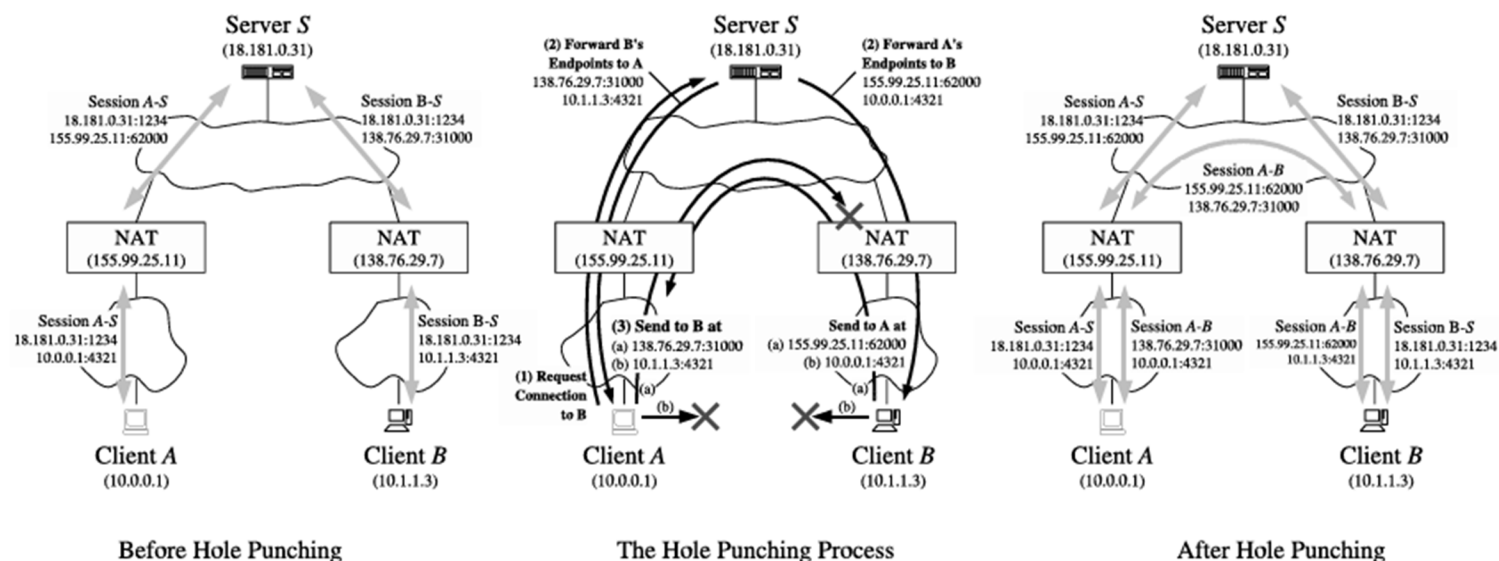


Figure 5: UDP Hole Punching, Peers Behind Different NATs

A and B each initiated UDP communication sessions from their local port 4321 to port 1234 on server S. In handling these outbound sessions, NAT A assigned port 62000 at its own public IP address, 155.99.25.11, for the use of A's session with S, and NAT B assigned port 31000 at its own public IP address, 138.76.29.7, to B's session with S. In A's registration message to S, A reported its private endpoint to S as 10.0.0.1:4321, where 10.0.0.1 was A's private IP address on its own private network. S recorded A's reported private endpoint, along with A's public endpoint as observed by S itself. A's public endpoint was 155.99.25.11:62000, the temporary endpoint assigned to the session by the NAT.

Similarly, when client B registered, S recorded B's private endpoint as

10.1.1.3:4321 and B's public endpoint as 138.76.29.7:31000. EX-1005 p. 5.

A and B each sent UDP datagrams directly to each of these endpoints. As A's outgoing message sent to B's public endpoint passed through A's NAT, this NAT noticed that this is the first UDP packet in a new outgoing session. The new session's source endpoint (10.0.0.1:4321) was the same as that of the existing session between A and S, but its destination endpoint was different. NAT A preserved the identity of A's private endpoint, and consistently translated all outbound sessions from private source endpoint 10.0.0.1:4321 to the corresponding public source endpoint 155.99.25.11:62000. A's first outgoing message to B's public endpoint thus, in effect, "punches a hole" in A's NAT for a new UDP session identified by the endpoints (10.0.0.1:4321, 138.76.29.7:31000) on A's private network (the network behind A's NAT), and by the endpoints (155.99.25.11:62000, 138.76.29.7:31000) on the main Internet. As this message traverses A's NAT, the NAT maps messages originating at 10.0.0.1:4321 to a destination of 138.76.29.7:31000, and vice-versa. EX-1005 p. 6.

If A's message to B's public endpoint reached B's NAT before B's first message to A had crossed B's own NAT, then B's NAT interpreted A's inbound message as unsolicited incoming traffic and dropped it—NATs do not automatically forward traffic sent to public endpoints to private endpoints. B's first

message to A's public address, however, similarly opened a hole in B's NAT, for a new UDP session identified by the endpoints (10.1.1.3:4321, 155.99.25.11:62000) on B's private network, and by the endpoints (138.76.29.7:31000, 155.99.25.11:62000) on the Internet. As this message traverses B's NAT, the NAT maps traffic originating from 155.99.25.11:62000 to a destination of 10.1.1.3:4321, and vice-versa. Once the first messages from A and B have crossed their respective NATs, holes are opened in each direction and UDP communication can proceed directly between A and B without assistance from S. This is because NATs A and B have created mappings between the appropriate public and private endpoints.

EX-1005 p. 6.

V. IDENTIFICATION OF HOW CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-10

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

Ground	Claims	Basis	Reference
1	1-10	35 U.S.C. §103	Pankratov

1. The Pankratov Reference

U.S. Patent Publication No. 2007/0157303 (“Pankratov”) (EX-1004) is titled “Server-Mediated Setup And Maintenance Of Peer-To-Peer Client Computer Communications”, and it published on July 5, 2007, from Pat. Appn. No. 11/642,272 filed on December 19, 2006, and claiming priority to provisional application 60/754,302 filed December 19, 2006. Pankratov qualifies as prior art under Pre-AIA 35 U.S.C. §102(b). Pankratov was not cited or applied by the examiner during prosecution of the Challenged Claims.

Pankratov is generally directed to virtual private networking, network traffic tunneling, and network traffic relaying between internet-connected VPN members (“nodes” and “computers”). EX-1004 [0005-0007], [0023]. Specifically, the method taught by Pankratov “improves and extends UDP hole punching technology such that the chances of successfully connecting two computers, each using a NAT device, significantly increases.” EX-1004 [0022].

“In general, this advantage is provided by a secure mediated peer-to-peer system that comprises a mediation server and end-node peer clients. The mediation server tracks client locations and provides mediation services required for establishing direct peer-to-peer tunnels between client nodes.”

EX-1004 [0023].

Pankratov terms this method “assisted NAT and firewall traversal (“ANFT”), although this designation should not be construed to limit the invention, which can be practiced in association with clients that access the Internet through any type of traffic policing device.” EX-1004 [0047]. “In general, preparing a connection setup between two client computers using ANFT preferably includes discovery, prediction and confirmation. . . .” EX-1004 [0059].

“Step (a) updates client address/port information for one or both clients. . . . [T]he mediation server performs this update by asking the given client to send a single probe to the mediation server or other backend machine. If the server(s) do not receive this probe in a given time, the mediation server assumes the probe packet was lost

Step (b) occurs if the IP/port needs to be predicted. . . . [T]he mediation server uses the information is [sic] has obtained during the earlier data collection processes to guess the next port the given client is going to use.

Step (c) prepares the tunnel In certain cases the mediation server will ask a given client to send a packet towards its peer.

Step (d), tunnel confirmation, is unconditional and is always executed. When a script reaches this step, the tunnel engine already knows what IP/port numbers both clients will be using towards each other; the mediation server uses this information to ask client A to send a probe to client B, and to ask client B to send a probe to client A. If, as described above, the mediation server then receives a probe reflection packet, the server has confirmed that the tunnel is operational in a respective direction. . . The mediation server then completes the setup sequence by notifying the clients.”

EX-1004 [0027]-[0030].

2. Detailed Application of Pankratov to the Challenged Claims

Claim 1

[1.0] A communication method that provides end-to-end communication in a virtual network environment, the method comprising:

To the extent that the preamble is limiting, Pankratov discloses a method that provides end-to-end communication in a virtual network environment. Specifically, Pankratov provides “a virtual private networking system that uses traditional VPNs, assisted NAT traversal (namely, UDP hole punching), proxy traversal (also known as HTTP and SSL tunneling), and/or relays.” EX-1004 [0038].

[1.1] a plurality of virtual tunnel routers comprising a first virtual tunnel router and a second virtual tunnel router receiving a message containing virtual network prefix information from a tunnel mapping controller;

Pankratov discloses that client computers [*virtual tunnel routers*] communicate with a server [*tunnel mapping controller*] to tunnel VPN traffic to/from other client computers through virtual networks. The client computers access a LAN or WAN and can operate as a server. EX-1004 [0040]. The client computers are responsible for emulating a LAN like environment on an end-user machine, communicating with the server and tunneling VPN traffic to/from other client computers through the virtual networks. EX-1004 [0107]. Pankratov further discloses that the client computer includes a virtual adapter. The virtual network adapter is an operating system component that appears as a physical network card to the system, but does not correspond to any actual hardware. Instead, preferably all traffic sent by the system to this adapter is forwarded to an application process. This process then inspects the traffic and either drops it (discards it) or forwards it to the other VPN member(s) via the tunnel(s). EX-1004 [0110].

Pankratov further discloses that a mediation server [*tunnel mapping controller*] is responsible for configuring client computers, and that as part of configuring, it provides each computer with virtual IP address and a non-trivial subnet that covers the entire virtual IP address range as configured on the server

[*receiving a message containing virtual network prefix information from a tunnel mapping controller*]. EX-1004 [0109], [0114]. The virtual adapter at the client computer is configured with the virtual IP address and the non-trivial subnet [*virtual network prefix information*]. The server uses the virtual IP address and the non-trivial subnet to group clients together. The mediation server decides which client computers require tunnels between themselves based on client grouping information. EX-1004 [0114]. Thus, a POSITA understood that the client computers would receive VPN traffic tunneled between VPN members for delivery to devices in their virtual sub-net and are therefore virtual tunnel routers.

Pankratov discloses that a mediation server (“server”) [*tunnel mapping controller*] provides mediation services to establish direct peer-to-peer tunnels between client computers. EX-1004 [0023]. The mediation server tracks client locations and provides mediation services required for establishing direct peer-to-peer tunnels between client nodes. EX-1004 [0071]. In one example, Pankratov discloses that if client A (in a first peer) desires to have a secure tunnel established to client B (a second peer), both A and B execute commands from the mediation server's tunneling engine. The clients need to register for the service to obtain the tunnel engine. A connection process begins when client A establishes a connection to one of the mediation servers. Client A goes through a discovery process to enable the mediation server to understand exactly how the client's NAT device

modifies the source port number when the packet passes through it from the LAN to the Internet. A similar discovery process may be carried for client B. Once discovery is complete, the mediation server knows each client's mapping/firewall type, and can generate a set of one or more scripts that will be used to carry out a tunnel setup sequence. EX-1004 [0072]. Thus, a POSITA understood that the mediation server is a *tunnel mapping controller*.

A POSITA understood a subnet to be a range of IP addresses associated with a network prefix to divide a larger network into smaller subnet. This understanding is consistent with Pankratov's disclosure that the virtual IP address and a non-trivial subnet covers a range of virtual IP addresses (EX-1004 [0114]), and is consistent with the disclosure of the '887 Patent that virtual network prefix information includes the IP addresses and subnet that covers a range of virtual IP addresses:

Virtual network prefix information is addresses assigned to terminals or devices connected to respective virtual networks. For example, if a virtual network has a prefix and length of 1.1.1.0/24, each terminal connected to the virtual network is assigned one IP in the range from 1.1.1.1 to 1.1.1.255, which is virtual network prefix information.

Ex-1001 6:48-53.

Thus, Pankratov discloses this limitation.

[1.2] determining whether the first virtual tunnel router has received a hole punching message from the second virtual tunnel router;

Pankratov discloses this limitation. Pankratov discloses that messages for hole punching are sent for the purposes of creating a mapping in the NAT device that allows an internal computer to start receiving traffic from the peers outside the NAT. EX-1004 [0018]. Pankratov discloses that the ANFT process extends traditional UDP hole punching to support NAT types and performs this process by sending messages in order to establish a tunnel. EX-1004 [0047].

Pankratov discloses that in one embodiment that the mediation server instructs the clients to go through a NAT type discovery process. The purpose of the discovery process is to enable the mediation server to understand exactly how the client's NAT device modifies (or “mangles”) the source port number and IP source address when the packet passes through it from the LAN to the Internet. By performing discovery, the mediation server can determine the NAT mangling logic, which in turn enables the server to more accurately predict the port that will be used to set up the peer-to-peer tunnel. EX-1004 [0025]. As a result of the discovery process, the mediation server now knows each clients’ mapping/firewall type. EX-1004 [0025]. In other words, through the discovery process, the mediation server learns the mapping between the virtual IP address and port and the external IP and address of a port of a client device.

Specifically, the ANFT discovery process includes client computer A sending a ping packet [*hole punching message*] to computer B's address. Computer B then sends a ping reflection packet to the server containing the external source address and the port of client computer A as determined by computer B using the ping packet and the data from the ping packet. EX-1004 [0048]. The server uses this exchange to learn the state of the port mappings between the internal and external addresses on the NAT devices in front of client computer A and/or to verify that computer B is reachable from client computer A at a certain IP address and port [*determining whether the first virtual tunnel router has received a hole punching message from the second virtual tunnel router*].¹ EX-1004 [0049].

Pankratov discloses that in a preferred embodiment the server again uses ping probing packets to instruct one or both client computers to communicate with the other, either sequentially or simultaneously, using the state of the port mappings the server learned or predicted based on received ping reflection packets. EX-1004 [0049], [0062]. It then observes the source information in the ping

¹ Pankratov discloses that the ping probing process can be performed for each client computer and thus either client A or client B can be the first virtual tunnel router, with the other being the second tunnel router.

reflection packets to validate and possibly correct the predicted port mappings and confirm the tunnel between the clients. Thus, in a preferred embodiment, the server asks client A to ping client B; likewise, the server asks client B to ping client A. The server then observes the source information in the reflection packets to confirm the tunnel. EX-1004 [0067].

Thus, a POSITA understood that Pankratov's ANFT process is a hole punching method where both computer A and B sending ping packets [*hole punching messages*] and the server determines whether a hole punching message was received at one client from the other client.

[1.3] if the first virtual tunnel router has received a hole punching message, the first virtual tunnel router establishing a tunnel with the second virtual tunnel router based on the virtual network prefix information; and

Pankratov discloses this limitation. Pankratov discloses that its ANFT method and system extends traditional UDP hole punching to support NAT types that are, for example, not identity-preserving. EX-1004 [0047]. As discussed with respect to limitation [1.2], the discovery process is used to learn the mapping of the IP addresses in order to establish a tunnel between client A [*first virtual tunnel router*] and client B [*second virtual tunnel router*]. Pankratov discloses that once discovery is complete, a confirmation step is used to activate the tunnel between the client computers based on the discovery step including the mapping of

the virtual IP addresses and subnets for client A and B [*virtual network prefix information*] to the external IP addresses of client A and B. [*if the first virtual tunnel router has received a hole punching message, the first virtual tunnel router establishing a tunnel with the second virtual tunnel router based on the virtual network prefix information*]. EX-1004 [0026], [0067]-[0069], [0110]. The confirmation step includes the server instructing one or both client computers to communicate with the other, either sequentially or simultaneously. It then observes the source information in the ping reflection packets to validate and possibly correct the prediction and confirm the tunnel between the clients. Thus, in a preferred embodiment, the server asks client A to ping client B; likewise, the server asks client B to ping client A. The server then observes the source information in the reflection packets to confirm the tunnel. EX-1004 [0067].

Tunnel creation utilizing ANFT may be employed by a server to create tunnels between clients in fully-meshed and hub-n-spoke networks. The server groups clients and decides which clients require tunnels between themselves. EX-1004 [0107], [0115]-[0116]. When clients are configured in preparation for network creation, the server assigns clients a virtual IP address and a subnet. EX-1004 [0108]. Each client then configures a virtual network adapter with a non-trivial subnet that covers the entire virtual IP address range as configured by the server. EX-1004 [0110], [0114]. When a client on the network sends a packet

through a tunnel, it uses its target's virtual IP address. When the target client receives the packet, the client's virtual network adapter passes the packet to the appropriate operating system. EX-1004 [0111]. The virtual network adapter may also forward the packet to other VPN member(s) via tunnel(s). EX-1004 [0110]. Thus, A POSITA would have understood that tunnels are established between clients based on the virtual network prefix information.

[1.4] the first virtual tunnel router performing direct communication with the second virtual tunnel router through the established tunnel.

Pankratov discloses this limitation. Pankratov discloses that if the tunnel setup protocol succeeds, the server provides each client with the IP address/port number of the other client so that the first client can start exchanging data with the second client directly through the tunnel and without passing through the server *[the first virtual tunnel router performing direct communication with the second virtual tunnel router through the established tunnel]*. EX-1004 [0031], [0070]. For example, Pankratov discloses that networks may be fully-meshed or hub-n-spoke. EX-1004 [0116]. In such networks, virtual network adapters provided to each client may receive packets and forward them to other VPN member(s) via tunnel(s). Clients may also utilize virtual network adapters to send packets to a target client using the target client's virtual IP address. EX-1004 [0110]-[0111]. Pankratov enables direct tunnels between members of a VPN. EX-1004 [0123].

Claim 2

[2.1] The method of claim 1, wherein the receiving of a message comprises: the first virtual tunnel router transmitting a registration request message to the tunnel mapping controller; and

Pankratov discloses this limitation. Pankratov discloses that , when the client computer is initially configured, it establishes a control session with the server EX-1004 [0109]. Pankratov further discloses that when the client computer is initially configured, it generates a cryptographic identity. It then establishes a control session with the server, secures it using cryptography mechanisms, authenticates the server and submits its public identity (public key) for registration [*the first virtual tunnel router transmitting a registration request message to the tunnel mapping controller*]. In return, the server allocates a virtual IP address and subnet for the client computer and sends it to the client computer. The virtual IP address/cryptographic identity pair becomes part of the client computer's login information. EX-1004 [0109], [0114]. In the example discussed above, both client A and B would register with the mediation server and the server would allocate a virtual IP address for each client computer and send it to the client computers. Pankratov further discloses that each client via its virtual adapter is configured with a virtual IP address and a non-trivial subnet that covers the entire virtual IP address range as configured on the server. EX-1004 [0114].

[2.2] if the first virtual tunnel router is a virtual router not registered in the tunnel mapping controller, the first virtual tunnel router receiving a response message containing virtual network prefix information created from the first virtual tunnel router from the tunnel mapping controller.²

Pankratov discloses this limitation. As discussed with respect to limitation [2.1], a client registers with the mediation server. In return, the server allocates a virtual IP address and subnet for the client computer and sends it to the client computer. The virtual IP address/cryptographic identity pair becomes part of the client computer's login information. The client computer uses the virtual IP address and subnet to configure a virtual network adapter [*the first virtual tunnel router receiving a response message containing virtual network prefix information created from the first virtual tunnel router from the tunnel mapping controller*]. EX-1004 [0114]. A POSITA understands that the login information would be stored at the server, and if a client that has not previously registered with server, i.e., it does not have login information, the server would allocate a virtual IP address and subnet for the client computer and send it to the client computer [*if the first virtual tunnel router is a virtual router not registered in the tunnel mapping controller*]. EX-1004 [0109], [0114].

² The patent owner interprets this claim to read “. . . information created ~~from~~ [for] the first virtual tunnel router. . . .” EX-1006, app. C, p. 31.

Claim 3

[3.1] The method of claim 2, comprising: if the first virtual tunnel router is a pre-stored virtual tunnel router and the first virtual tunnel router has moved, receiving an IP from a new virtual network to which the first virtual tunnel router has moved and registered;

Pankratov discloses this limitation. Pankratov discloses that a server in a virtual network registers a client computer in the virtual network by allocating a virtual IP address and cryptographic identity pair, which becomes part of the client computer's login information. EX-1004 [0109]. A POSITA understood that the login information is prestored at the server so that the client computer can log into and off of the virtual network as desired. *[if the first virtual tunnel router is a pre-stored virtual tunnel router]*. EX-1004 [0115].

A POSITA would understand that if the client computer moves to a new virtual network, the client computer needs to register with a server in the new virtual network to receive a new virtual IP address and cryptographic identity pair, which becomes part of the client computer's login information for the new virtual network *[and the first virtual tunnel router has moved, receiving an IP from a new virtual network to which the first virtual tunnel router has moved and registered]*. EX-1004 [0109].

[3.2] the first virtual tunnel router connecting to the new virtual network using the received IP;

Pankratov discloses this limitation. Pankratov teaches that once the client has obtained the virtual IP address and subnet, it uses it to configure a virtual network adapter. EX-1004 [0114]. The virtual network adapter is an operating system component that appears as a physical network card to the system, but does not correspond to any actual hardware. All traffic sent by the system to this virtual network adapter is forwarded to an application process in the client computer, and data is sent to a target in the virtual network using the target's virtual IP address [*the first virtual tunnel router connecting to the new virtual network using the received IP*]. EX-1004 [0110].

[3.3] the first virtual tunnel router connected to the new virtual network, transmitting a registration and information update request message to the tunnel mapping controller; and

Pankratov discloses this limitation. Pankratov that after the client is connected to the server, it send updated client address/port information. The mediation server performs this update by asking the given client to send a single probe to the mediation server [*the first virtual tunnel router connected to the new virtual network, transmitting a registration and information update request message to the tunnel mapping controller*]. EX-1004 [0027], [0072].

Therefore, Pankratov discloses this limitation.

[3.4] performing a tunnel creation procedure with virtual tunnel routers adjacent to the first virtual tunnel router.

Pankratov discloses this limitation. Pankratov discloses that when two peer nodes like client A and client B desire to have a secure tunnel established between them, both client A and B can execute the commands of the server's tunneling engine. EX-1004 [0025]. Pankratov discloses that the tunnel creation process begins using ANFT. ANFT uses a packet exchange method referred to as ping probing. In one embodiment ping probing includes three transmissions. In the first transmission, the server transmits a ping request packet to client computer A. The ping request packet contains the address and the port of the computer B and some data, where computer B has a communication channel to the server S. The next transmission is client computer A sending a ping packet to the computer B's address and with the payload (data) specified in the ping request packet. The third transmission is computer B sending a ping reflection packet to the server. The ping reflection packet contains the source address and the port of client computer A as determined by computer B using the ping packet and the data from the ping packet. EX-1004 [0048]. Likewise, the server may repeat ping probing originating with a ping request packet to computer B. The mediation server observes the source information in the reflection packets to confirm the tunnel and then activates the tunnel between the client computers using the predicted ports and to verify that the tunnel operates in both directions [*performing a tunnel creation procedure with virtual tunnel routers adjacent to the first virtual tunnel router*]. EX-1004 [0067].

Pankratov further discloses that the virtual network may be fully-meshed, which means that the tunnels are setup between all online network peers. EX-1004 0116]. Thus, in a fully meshed network, a POSITA understood that client A and client B would be *adjacent tunnel routers* connected by tunnels. Additionally, Pankratov discloses that the server decides which client computers require tunnels between themselves based on client computer grouping information. A POSITA understood that this grouping would include adjacent clients. EX-1004 [0115].

Claim 4

[4] The method of claim 3, wherein the performing of the tunnel creation procedure comprises the first virtual tunnel router connected to the new virtual network receiving adjacent virtual tunnel router information from the tunnel mapping controller.

Pankratov discloses this limitation for the same reasons as described with respect to limitation [3.4]. Specifically, the server transmits a ping request packet that contains the address and the port of the computer B, which is an adjacent tunnel router in a fully-meshed network [*wherein the performing of the tunnel creation procedure comprises the first virtual tunnel router connected to the new virtual network receiving adjacent virtual tunnel router information from the tunnel mapping controller*]. EX-1004 [0048], [0116].

Claim 5

[5.1] The method of claim 1, comprising: if the first virtual tunnel router has not received a hole punching message from the second virtual tunnel router, the first virtual tunnel router

performing a tunneling process with the tunnel mapping controller; and

Pankratov discloses this limitation. Pankratov discloses that a relay node controlled by the mediation server may be utilized if the ANFT tunnel setup protocol does not succeed [*if the first virtual tunnel router has not received a hole punching message from the second virtual tunnel router, the first virtual tunnel router performing a tunneling process with the tunnel mapping controller*]. EX-1004 [0031]-[0032]. Specifically, Pankratov discloses that a relay is used when the ANFT process fails, which a POSITA understood includes if the client computer does not receive a hole punching message from the second computer.³ EX-1004 [0091]-[0095].

Pankratov describes that in one embodiment the relay node may be a separate computer controlled by the server, but also describes that the server may comprise the relay node:

“A representative mediation server machine is a network-based server running commodity (e.g. Pentium-class) hardware, an operating

³ Pankratov discloses that the AFNT can be implemented with both client computers A and B sending hole punching messages to the other computer and thus either computer A or B can be the recited *first virtual tunnel router* and *second virtual tunnel router*. EX-1004 [0018].

system (e.g., Linux, Windows, OS-X, or the like), an application runtime environment (e.g., Java, ASP), and a set of applications or processes (e.g., applets or servlets, linkable libraries, native code, or the like, depending on platform), that provide the functionality of a given system or subsystem. As described, the service may be implemented in a standalone server, or across a distributed set of machines.”

EX-1004 [0129].

Thus, a POSITA understood that the relay may be included in the mediation server and thus if the hole punching is not successful the first virtual tunnel router performing a tunneling process with the tunnel mapping controller.

[5.3] when a tunnel is established between the first virtual tunnel router and the tunnel mapping controller, the first virtual tunnel router connecting the received virtual network prefix information to the tunnel.

As discussed with respect to limitation [1.1], Pankratov discloses that each client via its virtual adapter is configured with a virtual IP address and a non-trivial subnet that covers the entire virtual IP address range as configured on the server. EX-1004 [0114]. Thus, when a client is connected to tunnel, its adapter is linked to the tunnel so any traffic received by the client is delivered to the appropriate device associated with the virtual IP address and subnet *[when a tunnel is established between the first virtual tunnel router and the tunnel mapping controller, the first virtual tunnel*

router connecting the received virtual network prefix information to the tunnel]. EX-1004 [0110]-[0111].

Therefore, Pankratov discloses this limitation.

Claim 6

[6.0] A communication method that enables direct communication between a plurality of virtual tunnel routers including a first virtual tunnel router and a second virtual tunnel router by working in conjunction with a tunnel mapping controller, the method comprising:

Pankratov discloses this limitation for the same reasons as discussed with respect to limitations [1.0] and [1.1].

[6.1] the first virtual tunnel router and the second virtual tunnel router requesting virtual network prefix information from the tunnel mapping controller;

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [1.1] and [2.1]. Specifically, Pankratov discloses that when the client computer is initially configured, it establishes a control session with the server a client computer and in return, the server allocates a virtual IP address and subnet for the client computer and sends it to the client computer [*the first virtual tunnel router and the second virtual tunnel router requesting virtual network prefix information from the tunnel mapping controller*]. EX-1004 [0109]-[0110].

[6.2] the tunnel mapping controller generating virtual network prefix information of the first virtual tunnel router and second virtual tunnel router, respectively, and transmitting the same

along with information of a list of virtual tunnel routers for which previous connection information has been stored;

As discussed with respect to limitation [6.1], the server allocates virtual IP addresses and subnets to client computers. The client computer uses the virtual IP address and subnet to configure a virtual network adapter [*the tunnel mapping controller generating virtual network prefix information of the first virtual tunnel router and second virtual tunnel router, respectively, and transmitting the same*]. EX-1004, [0114] . EX-1004 [0114].

Pankratov discloses that the server decides which client computers require tunnels in virtual network that may be fully-meshed, which means that the server sets up tunnels between all online peers. EX-1004 [0115]-[0116]. Thus, the server stores and sends to each computer the IP address and ports of other computers to establish tunnels with the computer as discussed with respect to Claim 1. For example, in a fully-meshed or hub-n-spoke network, a computer Client A would receive the IP address and port of computer client B from the mediation server, along with the IP address and port of any other client computer that computer client A will establish a tunnel with [*along with information of a list of virtual tunnel routers for which previous connection information has been stored*]. EX-1004, [0115]-[0116]. Therefore, Pankratov discloses this limitation.

[6.3] the first virtual tunnel router and the second virtual tunnel router creating a tunnel; and

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [1.3].

[6.4] performing direct communication between the first virtual tunnel router and the second virtual tunnel router by linking the virtual network prefix information received by the first virtual tunnel router and the second virtual tunnel router, respectively.

Pankratov discloses this limitation for the same reasons as discussed with respect to limitations [1.4] and [5.2]. A client's virtual adapter preferably is configured with a virtual IP address and a non-trivial subnet that covers the entire virtual IP address range as configured on the server. EX-1004 [0114]. Pankratov discloses that the server decides which client computers require a tunnel between them and groups client computers based on virtual configuration information, e.g., virtual IP address and subnet. EX-1004 [0115]. Further, the virtual network adaptor at the server receives network traffic and forwards it directly to the appropriate client computer via a tunnel associated with the subnet of the client computer. EX-1004 [0110]. Thus, a POSITA understood that the virtual IP address and subnet for sending and receiving client computers were linked to a specific tunnel associated with the subnet. *[performing direct communication between the first virtual tunnel router and the second virtual tunnel router by linking the virtual network prefix information received by the first virtual tunnel router and the second virtual tunnel router, respectively.*

When the mediation server provides computer A and computer B with the other's IP address and port [*received by the first virtual tunnel router and the second virtual tunnel router*], the IP address and port of the two computers are linked to form a tunnel so that the first client can start exchanging data with the second client directly through the tunnel and without passing through the server [*performing direct communication between the first virtual tunnel router and the second virtual tunnel router*]. EX-1004 Claim 1.

Claim 7

[7.1] The method of claim 6, comprising: before requesting for the virtual prefix information, the first virtual tunnel router and the second virtual tunnel router transmitting a registration request message to the tunnel mapping controller;

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [6.1]. The registration request message also occurs on *every* client computer to register with the server. Pankratov teaches that “A connection process [between client computers] begins when client A establishes a connection to one of the mediation servers.” EX-1004 [0072], [0109], [0110]. Furthermore, client computers establish a secure control session with the server before submitting a public identity for registration. EX-1004 [0109]. Thus, Pankratov teaches that both client computers must transmit a registration request message prior to receiving any virtual network prefix information, and discloses this limitation.

[7.2] the tunnel mapping controller determining whether the first and second virtual tunnel routers are pre-stored virtual tunnel routers based on the transmitted registration request message; and

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [3.1]. Pankratov discloses that a connection process begins when client A establishes a connection to one of the mediation servers. If necessary, the mediation server instructs client A to go through a NAT type discovery process. EX-1004 [0025]. A POSITA understood that the discovery process is necessary if client A had not previously registered with the mediation server, since the mediation server uses this exchange to learn the state of the port mappings on the NAT devices in front of client computer A [*the tunnel mapping controller determining whether the first and second virtual tunnel routers are pre-stored virtual tunnel routers based on the transmitted registration request message*]. EX-1004 [0049]. This is further disclosed in Pankratov, which describes that a mediation server performs client presence tracking and location tracking which involves the client computers establishing sessions with the server to use the server's services. EX-1004 [0071], [0096]. Specifically, clients are assigned login information and may toggle their online presence individually. EX-1004 [0109], [0115]. Thus, a POSITA understood that Pankratov discloses that the

server pre-stores the IP address and port number for each client computer in order to perform presence and location tracking, and enable online presence toggling.

[7.3] if the first and second virtual tunnel routers are not pre-stored virtual tunnel routers, the tunnel mapping controller storing information contained in the registration request message and registering the first virtual tunnel router and the second virtual tunnel router.

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [7.2]. Specifically, if the IP address and port of the first and second computers are not stored at the mediation server, the server registers the computer and executes the discovery process. EX-1004 [0025], [0049], [0109].

Claim 8

[8.1] The method of claim 6, wherein the creating of a tunnel comprises: the first virtual tunnel router and the second virtual tunnel router transmitting and receiving a hole punching message based on the information of a list of virtual tunnel routers;

Pankratov discloses this limitation for the same reasons as discussed with respect to limitations [1.2] and [1.3]. Specifically, Pankratov teaches the ANFT process, which extends traditional UDP hole punching to support various NAT types and utilizes hole punching messages in order to establish a tunnel between computers. EX-1004 [0047]. Additionally, Pankratov further discloses that in a fully meshed network each computer establishes a tunnel with every other computer. EX-1004 [0116]. In order to do so, a POSITA understood that a hole

punching message must be exchanged between each pair of computers establishing a tunnel based on IP address and port information supplied by the mediation server *[based on the information of a list of virtual tunnel routers]*.

By way of further example, Pankratov teaches that in one embodiment, the server initiates tunneling based on client computer grouping information:

“The server decides which client computers require tunnels between themselves based on client computer grouping information. Client computers are grouped together using virtual network configuration objects. A client computer may belong to more than one network. The clients also have per-network online status, meaning that they can toggle their online presence for each network individually.”

EX-1004 [0115].

Pankratov also teach that “. . .the server completes a tunnel setup between two clients. . . .” EX-1004 [0117].

In other words, Pankratov teaches that hole punching messages between clients may be initiated by the server based on client grouping information, and discloses this limitation.

[8.2] determining whether the transmission and reception of the hole punching message between the first virtual tunnel router and the second virtual tunnel router are successful;

Pankratov discloses this limitation for the same reasons as described with respect to limitation [5.1]. Pankratov discloses that a relay is used when the ANFT process fails, which a POSITA understood includes determining if the tunnel setup protocol does not succeed [*determining whether the transmission and reception of the hole punching message between the first virtual tunnel router and the second virtual tunnel router are successful*]. EX-1004 [0031]-[0032], [0091].

[8.3] if anyone of the virtual tunnel routers fails in the transmission and reception of the hole punching message, the first virtual tunnel router and the second virtual tunnel router each establishing a tunnel with the tunnel mapping controller; and

Pankratov discloses this limitation for the same reasons as described with respect to limitation [5.1]. Pankratov provides a relay node controlled by the server that connects via tunnels to clients and provides communications via relay when direct client-to-client tunneling is unavailable. EX-1004 [0020], [0091-0095]. Furthermore, as discussed with respect to claim [5.1], the server may comprise the relay node in some embodiments. EX-1004 [0129].

[8.4] the first virtual tunnel router and the second virtual tunnel router each linking the received virtual network prefix information to the established tunnel.

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [6.4].

Claim 9

[9.1] The method of claim 6, comprising: when the second virtual tunnel router moves after the performing of direct communication, registering the second virtual tunnel router to a virtual network to which the second virtual tunnel router has moved, and receiving an IP from the virtual network;

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [3.1].

[9.2] the second virtual tunnel router transmitting a registration/information update request message containing the received IP to the tunnel mapping controller;

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [3.3].

[9.3] the tunnel mapping controller updating the information of the second virtual tunnel router with the virtual tunnel router information contained in the registration/information update request message;

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [3.3].

[9.4] the tunnel mapping controller searching for an adjacent virtual tunnel router having a tunnel established with the second virtual tunnel router; and

Pankratov discloses this limitation. Pankratov teaches that “[p]referably, the server also keeps track of all client computer pairs that have established tunnels with each other,” and that “[t]he server decides which client computers require tunnels between themselves based on client computer grouping information” [the

tunnel mapping controller searching for an adjacent virtual tunnel router having a tunnel established with the second virtual tunnel router]. EX-1004 [0099], [0115].

As discussed above with respect to claim [3.4] and [6.2], Pankratov discloses a service with as few as two peer nodes, and a fully meshed networked where all nodes (*i.e.*, “adjacent” peers) are connected by tunnels, capable of connection, and a server which is aware of network topology and adjacency. *See, e.g.*, 1004 [0115], [0116], and [0024].

Therefore, Pankratov teaches a tunnel mapping controller with the capability to search for adjacent virtual tunnel routers and maintain in memory a listed of established tunnels and discloses this limitation.

[9.5] the tunnel mapping controller transmitting the updated virtual tunnel router information to the searched adjacent virtual tunnel router.

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [4.0].

Pankratov teaches that during the tunnel establishment process, the server will send the information of one client to an adjacent peer and request the client message that adjacent peer, and vice versa:

“Step (d), tunnel confirmation, is unconditional and is always executed. When a script reaches this step, the tunnel engine already knows what IP/port numbers both clients will be using towards each other; the mediation server uses this information to ask client A to

send a probe to client B, and to ask client B to send a probe to client A.”

EX-1004 [0077].

Claim 10

[10] The method of claim 9, comprising, after the transmitting of the updated virtual tunnel router information, creating a tunnel between the second virtual tunnel router and the adjacent virtual tunnel router.

Pankratov discloses this limitation for the same reasons as discussed with respect to limitation [9.6]. Specifically, Step (c) prepares the tunnel, and Step (d) concludes with the server determining the tunnel is fully operational, and notifying the clients. EX-1004 [0076]-[0077]. When the tunnel is fully operational, Pankratov teaches that “client computers are provided with the other's confirmed external IP/port addresses and they may immediately start exchanging data through the tunnel.” EX-1004 [0069].

VI. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

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

Petitioner certifies that the real party-in-interest in this Petition is Cisco Systems, Inc.

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

1. Judicial Matters

To Petitioners' knowledge, the '887 Patent is involved in the following pending litigation:

Case Heading	Number	Tribunal	Date
<i>OptimNet LLC v. Cisco Systems, Inc.</i>	2-25-cv-00935	E.D. Tex.	Sept. 4, 2025

2. Administrative Matters

As of this Petition's filing and to the best knowledge of Petitioner, the '887 Patent has not been subject to any *inter partes* reviews, reissues or reexaminations.

3. Related Patents

To the best knowledge of Petitioner, there are no U.S. patents and patent applications related to the '887 Patent.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Back-Up Counsel
Patrick D. McPherson Reg. No. 46,255 PDMcpherson@duanemorris.com DUANE MORRIS LLP 901 New York Avenue NW Suite 700 East Washington, D.C. 20001 T: (202) 776-7800	Joseph A. Powers Reg. No. 47,006 JAPowers@duanemorris.com DUANE MORRIS LLP 30 South 17th Street Philadelphia, PA 19103-4196 T: (215) 979-1000 Patrick C. Muldoon Reg. No. 47,343 PCMuldoon@duanemorris.com DUANE MORRIS LLP

	901 New York Avenue NW Suite 700 East Washington, D.C. 20001 T: (202) 776-7800
--	---

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

Service via hand-delivery may be made at the postal mailing address of lead counsel. Petitioner consents to service by e-mail.

E. Payment of Fees – 37 C.F.R. §42.103

The required fee is being paid using the Patent Review Processing System.

VII. CONCLUSION

Petitioner requests the Board institute an IPR and cancel the Challenged Claims.

Respectfully submitted,

DUANE MORRIS LLP

Dated: March 27, 2026

/ Patrick D. McPherson /
Patrick D. McPherson
USPTO Reg. No. 46,255
DUANE MORRIS LLP
901 New York Avenue NW
Suite 700 East
Washington, D.C. 20001

LEAD COUNSEL FOR PETITIONER

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

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 8,925 words as calculated by the “Word Count” feature of Microsoft Word 365, the word processing program used to create it.

Dated: March 27, 2026

/ Patrick D. McPherson /

Patrick D. McPherson

Reg. No. 46,255

Lead Counsel for Petitioner

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 March 27, 2026, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent 8,780,887 and all supporting exhibits were served via Federal Express, postage prepaid, to the correspondence address of record for the '887 Patent:

Date of service March 27, 2026

Manner of service FEDERAL EXPRESS

Documents served Petition for *Inter Partes* Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 8,780,887; Petitioner's Exhibit List; All Exhibits; Petitioner's Power of Attorney.

Persons served 145742 - Paratus Law Group, PLLC
1765 Greensboro Station Place
Suite 320
Tysons Corner, VA
UNITED STATES

Courtesy copies of the Petition and supporting exhibits were sent by email to the litigation Counsel below:

Dale Chang
Email: dchang@raklaw.com
Kristopher Davis
Email: kdavis@raklaw.com
Bradley Hyde
Email: bhyde@raklaw.com

/s/Patrick C. Muldoon/
Patrick C. Muldoon
Reg. No. 47,343
Counsel for Petitioner