UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZOHO CORPORATION and ZOHO CORPORATION PVT., LTD.,
Petitioners,

v.

MEETRIX IP, LLC,
Patent Owner.

Case IPR2023-00382
Patent 9,843,612 B2

# PATENT OWNER'S NOTICE OF APPEAL

To the Director of the United States Patent and Trademark Office,

Pursuant to 35 U.S.C. §§ 141 and 142 and 37 C.F.R. § 90.2-90.3, notice is hereby given that Patent Owner Meetrix IP, LLC ("Patent Owner") appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision of the Patent Trial and Appeal Board ("Board"), entered on July 16, 2024 (Paper 26) in IPR2023-00382 regarding U.S. Patent No. 9,843,612 B2 ("the '612 Patent"), and from all underlying findings, orders, decisions, rulings, and opinions decided adversely to Patent Owner in the above-captioned proceeding.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Patent Owner states that the appeal will address all aspects of the Board's decision decided adversely to Patent Owner, including, without limitation, whether the Board erred in concluding that Petitioners have proven by a preponderance of the evidence that claims 19-29 of the '612 Patent are unpatentable; the Board's consideration of the expert testimony, prior art, and other evidence in the record; and the Board's factual findings, conclusions of law, or other determinations supporting or relating to the above issues. Patent Owner further reserves the right to challenge any finding or determination relating to the issues and matters listed above and to challenge any other issues or matters decided against Patent Owner in any order, decision, ruling, or opinion by the Board in the above-captioned proceeding.

Pursuant to 35 U.S.C. § 142 and 37 C.F.R. § 90.2(a), this Notice is being filed with the Director of the United States Patent and Trademark Office, and a

copy of this Notice is being concurrently filed with the Patent Trial and Appeal Board. In addition, a copy of this Notice is being filed with the Clerk of the United States Court of Appeals for the Federal Circuit, along with the applicable filing fee, via CM/ECF and pay.gov.

Date: September 17, 2024

Respectfully Submitted,

*/s/ Andrew G. DiNovo*
Andrew G. DiNovo
Reg. No. 40,115
DiNovo Price LLP
7000 North MoPac Expressway
Suite 350
Austin, TX 78731
Telephone: (512) 539-2625
Facsimile: (512) 727-6691

## CERTIFICATE OF FILING AND SERVICE

I hereby certify that, in addition to being filed electronically through the Patent Trial and Appeal Board's P-TACTS System, the original version of the foregoing PATENT OWNER'S NOTICE OF APPEAL was filed by Express Mail on September 17, 2024, with the Director of the United States Patent and Trademark Office, at the following address:

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

The undersigned also hereby certifies that a true and correct copy of the foregoing PATENT OWNER'S NOTICE OF APPEAL and the filing fee is being filed with the Clerk's Office for the United States Court of Appeals for the Federal Circuit on September 17, 2024 via the Court's CM/ECF filing system.

The undersigned also hereby certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing PATENT OWNER'S NOTICE OF APPEAL was served on counsel of record for Petitioners on September 17, 2024 at the email addresses listed below:

Hector J. Ribera
C.J. Alice Chuang
Carolyn Chang
Ryan J. Marton
Marton Ribera Schumann & Chang LLP
548 Market St., Suite 36117
San Francisco, CA 94104

hector@martonribera.com
cjalice@martonribera.com
carolyn@martonribera.com
ryan@martonribera.com

Dated: September 17, 2024

*/s/ Andrew G. DiNovo*

Andrew G. DiNovo
Reg. No. 40,115
DiNovo Price LLP
7000 North MoPac Expressway
Suite 350
Austin, Texas 78731

# ATTACHMENT A

Trials@uspto.gov
571-272-7822

Paper 26
Dated: July 16, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

ZOHO CORPORATION and ZOHO CORPORATION PVT., LTD.,
Petitioner,

v.

MEETRIX IP, LLC,
Patent Owner.

---

IPR2023-00382
Patent 9,843,612 B2

---

Before KARL D. EASTHOM, CHARLES J. BOUDREAU, and KARA L. SZPONDOWSKI, *Administrative Patent Judges*.

EASTHOM, *Administrative Patent Judge*.

DECISION
Final Written Decision
Determining All Challenged Claims Unpatentable
*35 U.S.C. § 314*

# I. INTRODUCTION

Zoho Corporation and Zoho Corporation Pvt., Ltd, Petitioner, filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 19–29 of U.S. Patent No. 9,843,612 B2 (Ex. 1001, the "'612 patent"). Pet. 1. Meetrix IP, LLC, Patent Owner, did not file a preliminary response.

After the Institution Decision (Paper 6, "Inst. Dec."), Patent Owner filed a Response (Paper 10, "PO Resp.") with a Declaration of Thomas Dye (Ex. 2001), Petitioner filed a Reply (Paper 13, "Reply"), and Patent Owner filed a Sur-reply (Paper 15). After the briefing, the Board conducted an oral hearing (involving this *inter partes* review and the other five concurrent and related *inter partes* reviews listed below as Related Matters) and entered a Transcript thereof in the record. Paper 25 ("Tr.").

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner demonstrates by a preponderance of evidence that challenged claims 19–29 of the '612 patent are unpatentable.

# II. BACKGROUND

## *A. Real Parties in Interest*

The parties identify themselves as the real parties in interest. Pet. 2; Paper 3, 2.

## *B. Related Matters*

Petitioner challenges claims 10–18 of the '612 patent in IPR2023-00380. IPR2023-00380, Paper 1. The parties identify the following district court proceedings as related matters involving the '612 patent or related patents: *Meetrix IP, LLC v. Zoho Corp.*, No. 6:21-cv-01288 (W.D. Tex.) (filed Dec. 10, 2021); *Meetrix IP, LLC v. Verizon Commc'ns, Inc.*, No. 6:21-cv-01289 (W.D. Tex.) (filed Dec. 10, 2021). *See* Pet. 3; Paper 3, 2.

Patent Owner identifies the following concurrent *inter partes* reviews as involving related patents challenged by Petitioner: IPR2023-00371, IPR2023-00377, IPR2023-00378, and IPR2023-00379. Paper 3, 2.

The '612 patent was the subject of two petitions for *inter partes* review filed by Cisco Systems, Inc. in proceedings that the Board dismissed prior to any institution decision pursuant to settlement. *See* IPR2019-00543, Papers 2, 8; IPR2019-00544, Papers 2, 8.

*C. The '612 Patent*

The '612 patent relates to "[a] system and method for supporting a multi-participant voice conference call using [Public Switched Telephone Network (PSTN)] and Internet networks." Ex. 1001, code (57). The method

> includes receiving voice from a PSTN client. The method also includes receiving voice data from a moderator and from at least one remote client connected to the Internet. The method then proceeds to mix the voice data from the PSTN client with the voice data from the moderator into a first mixed voice data that is transmitted to the remote client that is connected to the Internet. The method also mixes the voice data from the moderator with the voice data from the remote client connected to the Internet into a second mixed voice data that is transmitted to the PSTN client.

*Id.*

Figure 3 follows:

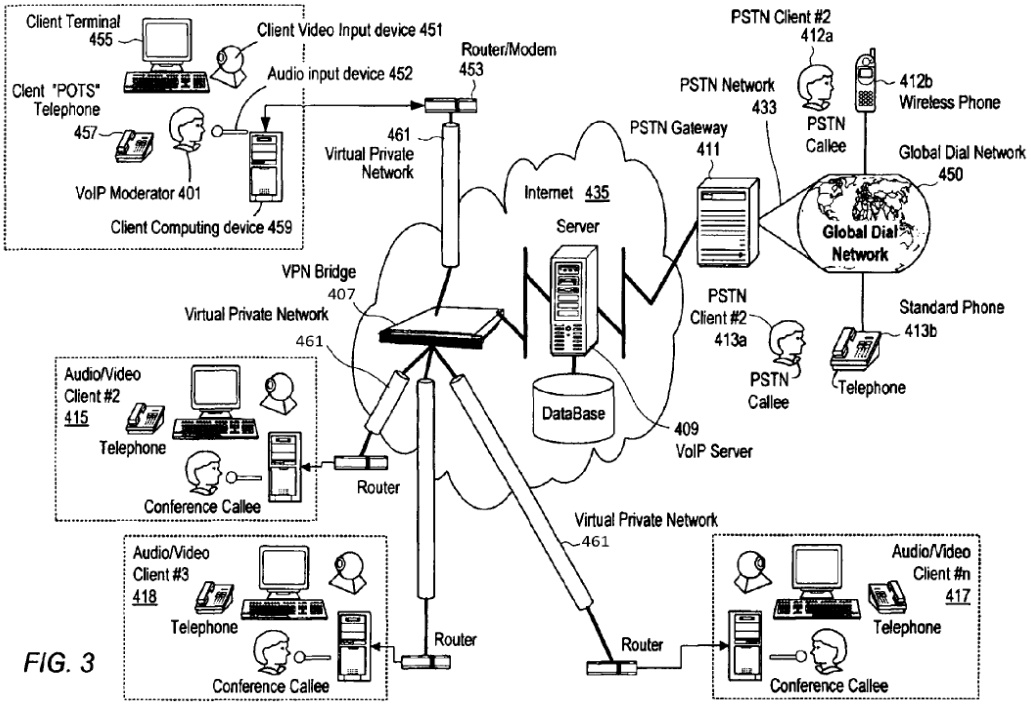



FIG. 3

Figure 3 depicts clients, including local moderator client 401, PSTN clients 412, 413, and remote Internet audio video clients 415, 417, and 418. Ex. 1001, 5:21–27, 7:17–38. The audio video clients "connect[] through routers or modems 453 preferably in a virtual private network [(VPN)] configuration 461" with "VPN bridge 407" located in the center of a "star topology," with connections to the VPN bridge serving as a "VPN tunnel." *Id.* at 5:1–13, 5:22–25, 5:45–48. The PSTN network includes "telephony clients using standard wired 413 or wireless telephone 412 systems," and connected to the Internet clients via PSTN gateway 411. *Id.* at 5:14–33.

The remote Internet clients share audio/video data through the VPN tunnels. Ex. 1001, 5:34–59; *see also id.* at Fig. 4. The PSTN clients share audio with the Internet clients. *Id.* at 9:24–44. The local moderator client "may . . . be the initiator of the meeting" and may initiate a "dial out for audio conferencing to the PSTN client." *Id.* at 7:22–26. Alternatively, a

"'Dial-in' may be used in addition using the same techniques . . . but in a reverse path scenario." *Id.* at 7:55–57. "The local moderator 401 and the remote audio video clients 418 may share audio and video data in a full duplex mode among . . . all participants with the exception of the PSTN client 412." *Id.* at 7:26–29.

The system also performs encoding and decoding of audio data using codecs of the prior art H.323 standard and the transmission of collaboration data per the prior art T.120 standard. Ex. 1001, 2:63–3:1, 3:17–22 ("[T]he H.323 recommendation defines a data collaboration capability as known and outlined in the T.120 data collaboration unit 225.").

### *D. Illustrative Claim*

Independent claim 19 is illustrative of the challenged claims, and follows (with bracketed information conforming to Petitioner's notation):

> 19. [19.P] A method for conducting a secure multi-participant conference call including full duplex audio, the method comprising:
>
> [19.1.1] receiving first audio data, first video data, and first collaboration data at a server from a first remote client [19.1.2] through a first Virtual Private Network (VPN) tunnel;
>
> [19.2.1] receiving second audio data at the server from a second remote client [19.2.2] through a second VPN tunnel;
>
> [19.3] receiving third audio data at the server from a Public Switched Telephone Network (PSTN) client through a PSTN gateway;
>
> [19.4] mixing the first audio data with the second audio data into a first mixed audio data;
>
> [19.5] mixing the second audio data with the third audio data into a second mixed audio data;
>
> [19.6] mixing the first audio data with the third audio data into a third mixed audio data;
>
> [19.7] transmitting the first mixed audio data from the server to the PSTN client through the PSTN gateway;

[19.8] transmitting the second mixed audio data from the server to the first remote client through the first VPN tunnel;

[19.9] transmitting the third mixed audio data from the server to the second remote client through the second VPN tunnel; and

[19.10] transmitting the first video data and the first collaboration data from the se[r]ver to the second remote client.

*E. Asserted Grounds of Unpatentability*

Petitioner contends that claims 19–29 are unpatentable as follows:[1]

| Claim(s) Challenged | 35 U.S.C. § | Reference(s)/Basis |
|---|---|---|
| 19–21, 25–27 | 103(a) | Knappe,[2] Elliott,[3] VPN Textbook,[4] Hendricks[5] |
| 22–24, 28, 29 | 103(a) | Knappe, Elliott, VPN Textbook, Hendricks, Drell[6] |

Pet. 4. Petitioner supports its Petition with a Declaration of Dr. Henry H. Houh. Ex. 1003.

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. § 103, effective March 16, 2013, which is after the '612 patent's effective filing date, Mar. 10, 2003 or March 9, 2004. *See* Ex. 1001, codes (60, 63). Therefore, the pre-AIA version of § 103 applies for purposes of institution.

[2] US Patent No. 7,180,997 B2, issued Feb. 20, 2007, filed Sept. 6, 2002. Ex. 1006.

[3] US Patent No. 6,690,654 B2, issued Feb. 10, 2004, filed Oct. 1, 1998. Ex. 1007.

[4] Excerpts from Jim Guichard & Ivan Pepelnjak, MPLS AND VPN ARCHITECTURES (2001). Ex. 1010.

[5] PCT Pub. No. WO 01/18665 A1, published Mar. 15, 2001. Ex. 1040.

[6] US Patent No. 7,089,285 B1, issued Aug. 8, 2006, filed Oct. 5, 2000. Ex. 1008.

## III. ANALYSIS OF THE GROUNDS

### *A. Legal Standards*

> Section 103(a) forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

*KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a)). The obviousness question involves resolving underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and when presented (not so here), (4) objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

### *B. Level of Ordinary Skill in the Art*

Determining whether an invention would have been obvious under 35 U.S.C. § 103 requires resolving the level of ordinary skill in the pertinent art at the time of the effective filing date of the claimed invention. *Graham*, 383 U.S. at 17. The person of ordinary skill in the art is a hypothetical person who knows the relevant art. *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Factors in determining the level of ordinary skill in the art include the types of problems encountered in the art, the sophistication of the technology, and educational level of active workers in the field. *Id.* One or more factors may predominate. *Id.*

Petitioner contends as follows:

> The subject matter of the '612 patent generally relates to the technical field of audio/video conferencing systems. A Person of Ordinary Skill in the Art ("POSITA") in March 2003

> would have had a working knowledge of the conferencing art. Ex_1003, ¶27. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and three or more years of professional experience relating to conferencing systems in packet-based networks, or without said professional experience, further education relating to conferencing systems in packet-based networks. *Id.* ¶¶24–27.

Pet. 7.

Patent Owner "believes a POSITA would have a bachelor's degree in electrical engineering, computer science, or equivalent with two years or more of experience in computing systems development." PO Resp. 12 (citing Ex. 2001 ¶ 3). The two proposals largely overlap.

Based on a review of the record, we adopt Petitioner's proposed level of ordinary skill in the art because it is consistent with the evidence of record, including the asserted prior art and '612 patent specification, except that we delete the qualifier "or more" in the phrase "three or more years" to eliminate vagueness as to the stated amount of professional experience. However, even if we were to adopt Patent Owner's proposal, we agree with the parties that the outcome would be the same. *See* Reply 2 (Petitioner arguing that "under either definition the result is the same"); Tr. 49:11–14 (Patent Owner contending that as to defining a "person of ordinary skill in the art," he "can't point to a material difference that would change the outcome of this" trial).

### *C. Claim Construction*

In *inter partes* reviews, the Board interprets claim language using the district-court-type standard, as described in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b). Under this standard, claim terms have their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art at the time of the

invention, in light of the language of the claims, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1313–14.

Petitioner relies on the ordinary and customary meaning under *Phillips*. Pet. 7–8. Patent Owner agrees that the *Phillips* standard applies and cites to a district court claim construction order, which lists thirteen claim constructions for patents related to the '612 patent and the '612 patent. PO Resp. 12–14 (citing Ex. 2002). Petitioner asserts the district court litigation involved "another party." *See* Reply 2.

Patent Owner "asserts that the claim terms should be construed consistently with Exhibit 2002, and that the challenged claims clearly do not read on the prior art under the proper claim construction." PO Resp. 13. Patent Owner does not specify what it deems "the proper claim construction" and does not explain why Petitioner's showing is not consistent with any particular claim construction from the district court. *See id.* at 12–14.

In any event, even if Exhibit 2002 includes construction of a claim term at issue here, we determine below that Petitioner shows that the challenged claims would have been obvious under constructions consistent to any such terms proposed by Patent Owner.[7] Moreover, as Petitioner argues, "Patent Owner arguments do not actually rely on any of these claim constructions," and "only a handful of the listed terms actually appear in the claims of the '612 patent." Reply 2. In its Sur-reply, Patent Owner does not direct attention to any dispositive issue that turns on the district court claim construction. Sur-reply 2.

[7] As discussed below, Patent Owner presents an argument related to the district court claim construction of "VPN 'tunnel.'" *See* Ex. 2002, 13.

Because any explicit construction would not alter the outcome, an explicit construction for any claim term is not necessary. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (stating that "we need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

*D. Obviousness, Claims 19–21 and 25–27*

Petitioner asserts that claims 19–21 and 25–27 would have been obvious under 35 U.S.C. § 103(a) based on the combined teachings of Knappe, Elliott, VPN Textbook, and Hendricks. Pet. 4. Patent Owner asserts, *inter alia*, that Petitioner does not show the obviousness of implementing a VPN tunnel with mixed audio data and also asserts that certain references do not disclose collaboration data and other features, as outlined below.

*1. Knappe (Ex. 1006)*

Knappe "relates generally to the field of multiparty communications." Ex. 1006, 1:8–9. Knappe's "method includes processing the plurality of participant voice streams and the moderator voice stream such that the intelligibility of the moderator voice stream is enhanced relative to at least one of the participant voice streams." *Id.* at 2:7–11.

Knappe's Figure 1 follows:

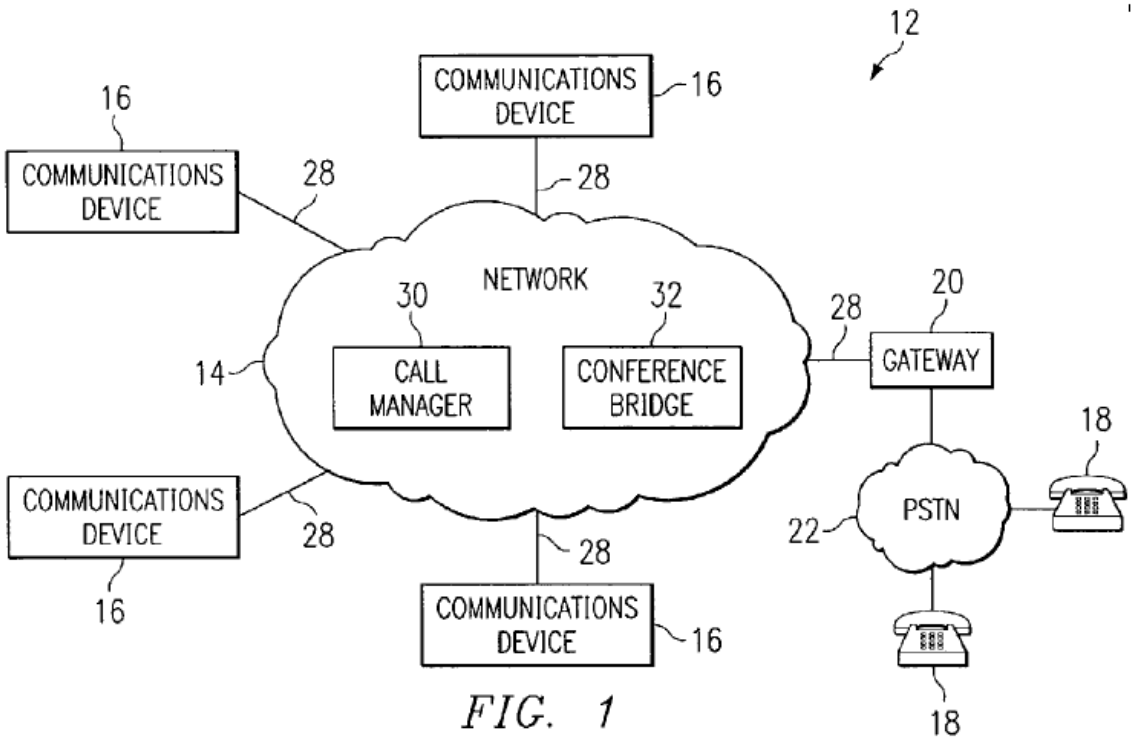



*FIG. 1*

Figure 1 is a block diagram of Knappe's communication system 12, which "includes a network 14 connecting a plurality of communication devices 16 to each other and to standard analog telephones 18 through a gateway 20 and the public switched telephone network (PSTN) 22." Ex. 1006, 3:41–45. "[C]all manager 30 controls the conference bridge 32 to set up, process and tear down conference calls and other multiparty communication sessions." *Id.* at 5:29–31. "The call manager 30 and the conference bridge 32 may be located in a central facility or have their functionality distributed across and/or at the periphery of the network 14." *Id.* at 4:30–33.

Under control of call manager 30, "conference bridge 32 provides real-time multiparty audio connections between three or more participants." Ex. 1006, 5:42–44. "[T]he conference bridge 32 receives media from participating devices 16 and, using suitable signal processing techniques, mixes the media to produce conference signals." *Id.* at 4:63–66. In other

words, "[d]uring the multiparty communications sessions, participants are connected and stream media through the conference bridge 32." *Id.* at 5:31–33.

"In accordance with a particular embodiment, network 14 is the Internet, a wide area network (WAN), a local area network (LAN) or other suitable packet-switched network." Ex. 1006, 3:50–53. Communication devices 16 include all types of IP (internet protocol) or other digital telephones, computers, PDAs, etc., and also include a "telephone 18 and gateway 20 combination capable of communicating real-time audio, video and/or other information over the network 14." *Id.* at 3:62–4:1. "[C]ommunication devices 16 also communicate control information with the network 14 to control call setup, teardown and processing as well as call services." *Id.* at 4:2–4. "[M]ultiparty communications sessions includ[e] real-time audio streams and/or video streams." *Id.* at 5:46–47.

Knappe's Figure 2 follows:

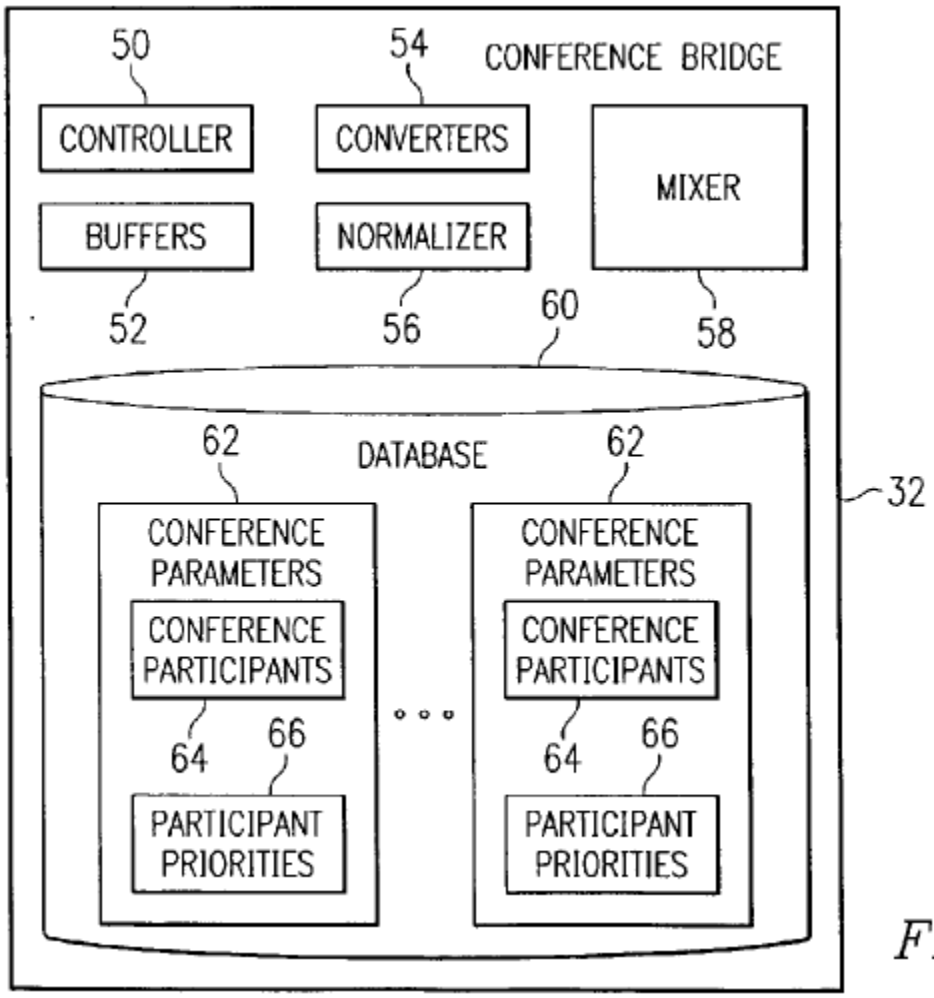



*FIG. 2*

As illustrated in Figure 2, Knappe's conference bridge 32 includes mixer 58. "[M]ixer 58 includes a plurality of summers or other suitable signal processing resources each operable to sum, add or otherwise combine a plurality of input streams into conference output streams for participants to a conference call." Ex. 1006, 6:33–37.

Knappe's Figure 3 follows:

FIG. 3

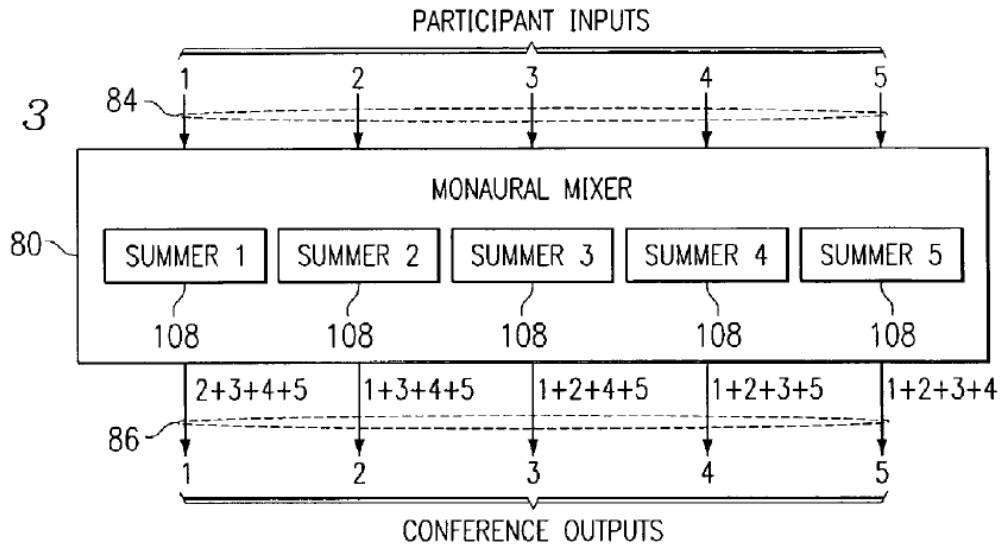



Figure 3 above represents an embodiment of Knappe's mixer 58 (*supra* Figure 2) in the form of monaural mixer 80. Ex. 1006, 6:52–55. "[M]onaural mixer 80 receives participant input streams 84 and combines the streams in summers 82 to generate conference output streams 86 for each participant to a conference call." *Id.* at 6:59–62. In one embodiment, a summer 82/108 assigned to each participant "receives audio input streams from each other participant to the conference call," and "combines the audio input streams to generate a conference output stream for delivery to the participant." *Id.* at 6:63–67.[8]

[8] Knappe refers to "summer 108" in connection with Figure 7 and "summers 182" in connection with Figure 3, although Figure 3 shows summers 108. *Compare* Ex. 1006, 8:24–26, *with* 6:59–63.

*2. Elliott (Ex. 1007)*

Elliott relates to a "method of communicating with a plurality of remote parties allows for multi-media collaboration." Ex. 1007, code (57). "Multi-media collaboration refers to the use of more than one media stream (e.g.: voice, fax, data, video, etc.) used in collaboration with more than one party." *Id.* at 2:66–3:1.

Elliott's Figure 1 follows:

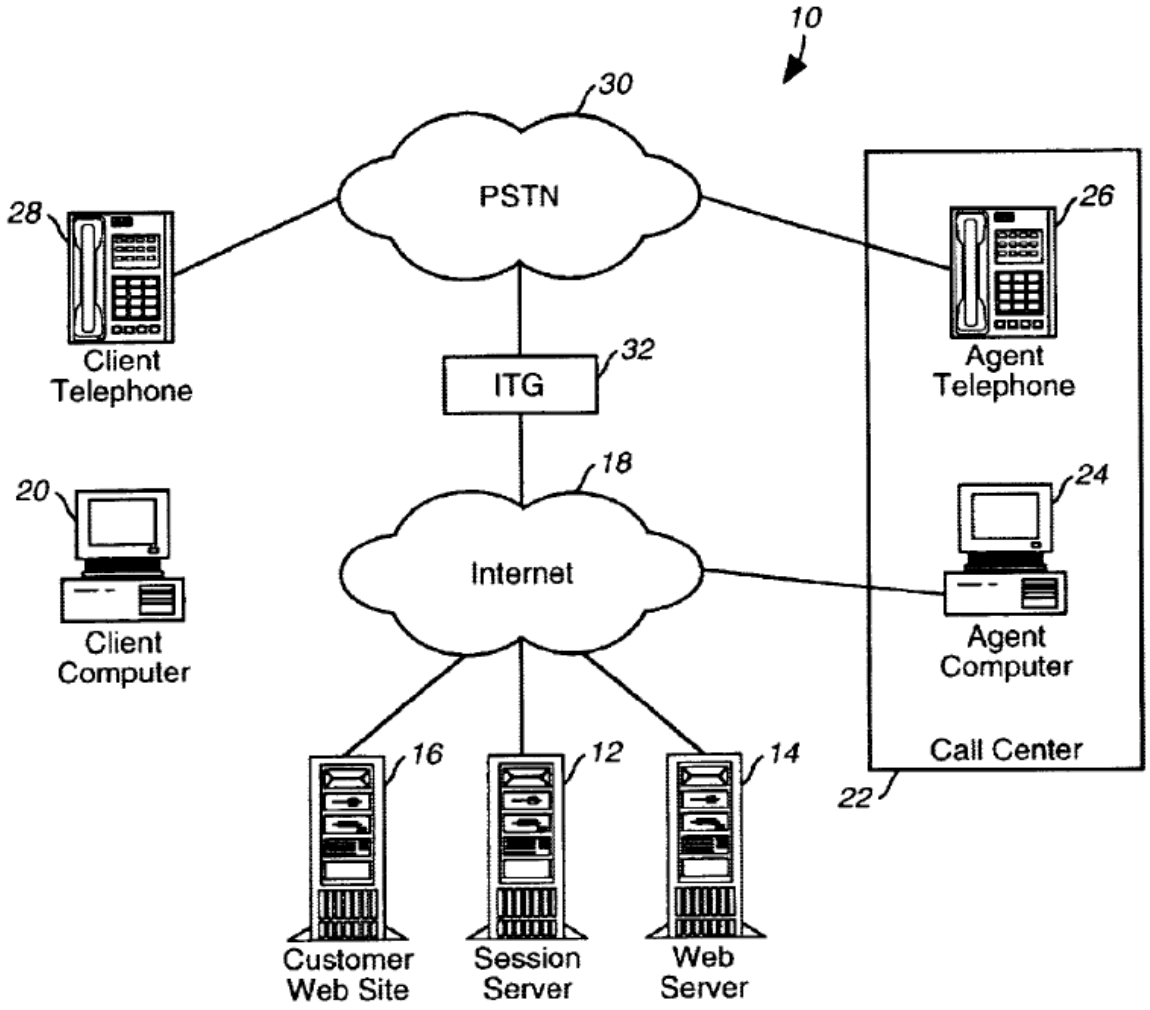



**FIG. 1**

Figure 1 illustrates network architecture 10 for using shared network resources by client computers 20 and client telephone 28 connected by

network 18, including "customer web site 16," "session server 12[,] and a web server 14 to provide services for a plurality parties such as call centers, agents, and clients." Ex. 1007, 3:57–63. "The 'client' is the party or parties which desire communication with the call center 22." *Id.* at 4:53–54. "[C]lient computer 20 could be connected to a corporate intranet which includes a gateway to the Internet." *Id.* at 5:31–33. "Client computer 20 may also be equipped with other software such as Internet telephone software, for placing Internet telephony calls. A client may also have a traditional telephone 28 for placing calls to call center agents over the public switched telephone network (PSTN) 30." *Id.* at 5:34–39.

Network 18 includes a variety of networks, including "the public Internet," "an exemplary Internet Protocol-based (IP-based) network 18 for multi-media collaboration." Ex. 1007, 4:10–12. Elliott also describes use of a VPN over public Internet network 18 or other network types, as follows:

> Network 18 could also comprise other IP-based networks as well as other networks. For example, network 18 could comprise an internet which is not connected to the public Internet. In this context, an "internet" (lowercase "i") is any collection of separate physical networks, interconnected by a common protocol, to form a single logical network. An internet would preferably, but not necessary use Internet Protocol. An internet which is owned by a single entity sometimes referred to as an intranet. Network 18 can comprise an intranet, which is or is not connected to the Internet. For example, network 18 can be either a public or a carrier supported virtual private network (VPN) or local area network (LAN) which uses IP or IP-tunneling. Other protocols can alternatively be utilized.

*Id.* at 4:20–24.

Elliott generally discloses "[m]ulit-media collaboration." Ex. 1007, 2:66. "Multi-media collaboration refers to the use of more than one media stream (e.g.: voice, fax, data, video, etc.) used in collaboration with more

than one party." *Id.* at 2:66–3:1. Some "examples of multi-media collaboration" include "multi-party conferencing," and "virtual private networks." *Id.* at 3:1–6. Elliott's "system and method of the present invention can also enable services for one-to-many and many-to-many IP-based collaboration." *Id.* at 3:13–15.

*3. VPN Textbook (Ex. 1010)*

VPN Textbook generally describes VPN (virtual private network) topologies for different networks. Ex. 1010, 115 (Chapter 7 heading page), 129.[9] VPN Textbook notes that "VPN is a concept that is more than 10-years old and is well known in the service provider market space." *Id.* at 115.

According to VPN Textbook, "[t]he most commonly encountered topology is a hub-and-spoke topology, where a number of remote offices (spokes) are connected to a central site (hub), similar to the setup in Figure 7-10." Ex. 1010, 129.

Figure 7-10 follows:

[9] Following Petitioner's usage, we cite the original page numbers at the top left and right corners of VPN Textbook's pages rather than the page numbers added by Petitioner in the lower right corner of the pages.

**Figure 7-10** *Hub-and-spoke Topology*

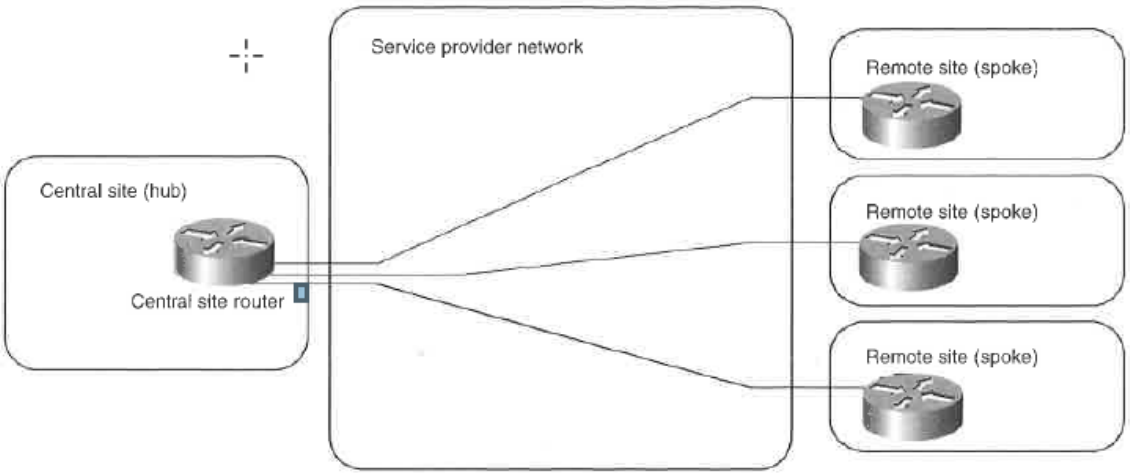



Figure 7-10 shows a central site (hub) router connected in a hub-and-spoke topology over service provider network lines secured by VPN technology and terminated at three different remote sites (spokes). *See id.* at 129–30. VPN customers often choose "the hub-and-spoke topology for cost or complexity reasons." *Id.* at 129 (Note).

VPN Textbook states that "it's no surprise that more and more business-to-business traffic takes place over the Internet." Ex. 1010, 119. Accordingly, the security solution involves using "encryption or one-time passwords" on an "end-to-end basis," for example as depicted below in Figure 7-3 (*id.*):

**Figure 7-3** *Typical Extranet Setup*

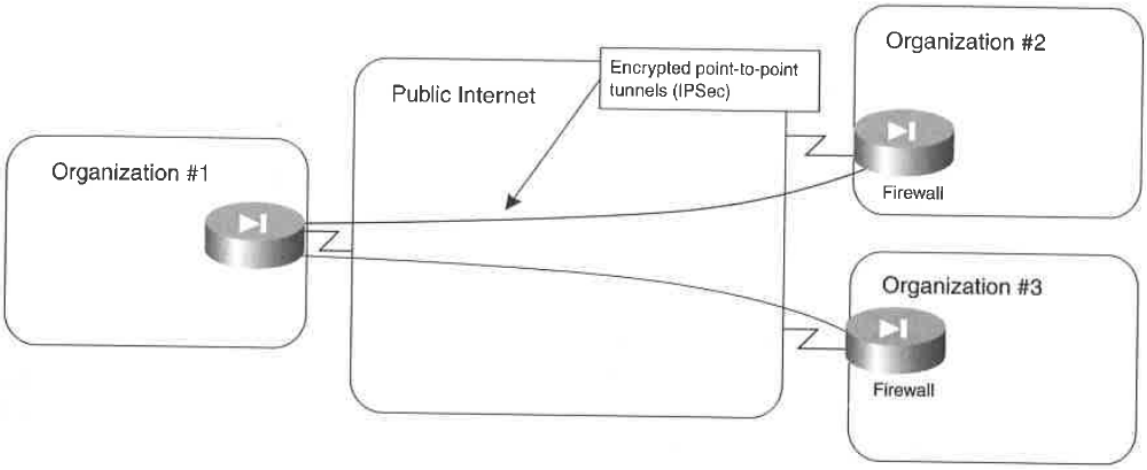



Figure 7-3 above illustrates a typical solution for Internet security by encrypting packets in "point-to-point tunnels" over the Internet for communications between organizations 1 and 2, and 1 and 3, with firewalls further protecting the networks within organizations 2 and 3. *See id.* at 117 (Packet Assembly and Disassembly), 119 (Fig. 7–3).

*4. Hendricks (Ex. 1040)*

Hendricks relates to a system for performing conference calls for multiple parties, "preferably video conference calls." Ex. 1040, code (57). The system provides for "duplex calls," as follows:

> one or a combination of several types of media (e.g., voice only or voice plus video and/or other media such as data, programs, etc.), and includes one-way broadcast calls . . . as well as full duplex calls or mixed media combinations of one-way broadcast and full duplex (e.g., broadcast video from one party and shared return audio from all parties).

*Id.* at 3:6–10.

*5. Claim 19*

In summary, method claim 19 requires, *inter alia*, establishing a conference call involving a server and three participants, specifically a first

remote client, a second remote client, and a PSTN client. The first remote client sends audio, video, and collaboration data to the server over a first VPN tunnel, the second remote client sends audio data to the server over a second VPN tunnel, and the PSTN client sends audio data to the server via a PSTN gateway. The method further requires mixing the audio data from two of the clients and transmitting it to the other of the clients for each of the three clients, wherein the server sends first mixed audio data to the PSTN client via the PSTN gateway, and sends second and third mixed audio data over the first and second VPN tunnels to the first and second remote clients, respectively.

*a) Preamble 19.P*

The preamble of claim 19 recites "[a] method for conducting a secure multi-participant conference call including full duplex audio, the method comprising." Petitioner relies on the combined teachings of Knappe, Elliott, the VPN Textbook, and Hendricks to address the preamble. *See* Pet. 27–29 (citing Ex. 1003 ¶¶ 353–361, 379–385).

First, Petitioner quotes Knappe as disclosing "multiparty communications, and more particularly [] a method and system for improving the intelligibility of a moderator during a multiparty communication session," wherein "[s]uch communication networks also allow multiple people to participate in . . . a 'conference call.'" Pet. 27 (alterations in original) (quoting Ex. 1006, 1:8–27). Petitioner relies on Knappe's Figure 1 (*see supra* § III.D.1) and contends that it "shows 'communication devices 16' that 'comprise IP or other digital telephones . . . cell or other mobile telephones or handset or any other device or set of devices such as the telephone 18 and gateway 20 combination capable of communicating real-time audio, video and/or other information over the

network 14.'" *Id.* at 28 (alteration in original) (quoting Ex. 1006, 3:62–4:1).[10]

Second, Petitioner contends that Knappe implies that its conference calls include full-duplex audio, because "Knappe teaches that the conference participants communicate with each other through conference bridge 32, which mixes the audio from other participants while excluding the audio of the participant that receives the mixed audio. Ex_1006, 6:59–7:11 ('During normal operation, each participant receives the audio input of each other participant. Thus, for example, the conference output stream of participant 1 includes the audio inputs of participants 2–5.'); Ex. 1003 ¶¶ 387–388)." Pet. 28–29. Based on Knappe's teachings, Petitioner contends that "[a] POSITA would recognize this simultaneous transmission and reception as a conference call that includes full-duplex audio." *Id.* at 29 (citing Ex. 1003 ¶¶ 387–388).

Third, Petitioner relies on Hendricks as teaching "full duplex calls" and "full duplex interconnectivity" for conference calls. Pet. 29 (quoting Ex. 1040, 3:8, 17:21; citing Ex. 1040, 27:12–19; Ex. 1003 ¶¶ 197, 389). Therefore, according to Petitioner, "[i]t would have been obvious for a POSITA to utilize full duplex audio in Knappe's system (as Hendricks teaches) because doing so would provide the participants of Knappe's communication devices 16 and telephones 18 a more natural way to communicate with each other during the conference." *Id.* (citing Ex. 1003 ¶¶ 371–378, 390; Ex. 1041, 1:20–39; Ex. 1042, 7:14–34).

[10] "IP" is an acronym for the Internet Protocol, which at its inception involved IP packets that include source and data addresses in headers and other fields. *See, e.g.*, Ex. 1003 ¶¶ 76, 81.

Finally, addressing the "secure" aspect of the preamble, Petitioner contends that "Elliott supplements Knappe and teaches using VPN tunneling for securing communications over a public network like the Internet." Pet. 28 (citing Ex. 1007, 4:6–12; Ex. 1003 ¶¶ 194–195, 353–361, 386). Therefore, Petitioner contends "[i]t would have been obvious to use in Knappe the VPN tunneling as taught in Elliott to secure communications over Knappe's Internet network 14." *Id.* (citing Ex. 1003 ¶¶ 194–195, 353–361 (relying on Elliott and VPN Textbook, Ex. 1010), 386). Petitioner discusses the VPN tunnel limitation in connection with limitations 19.1.2 and 19.2.1 as discussed below.

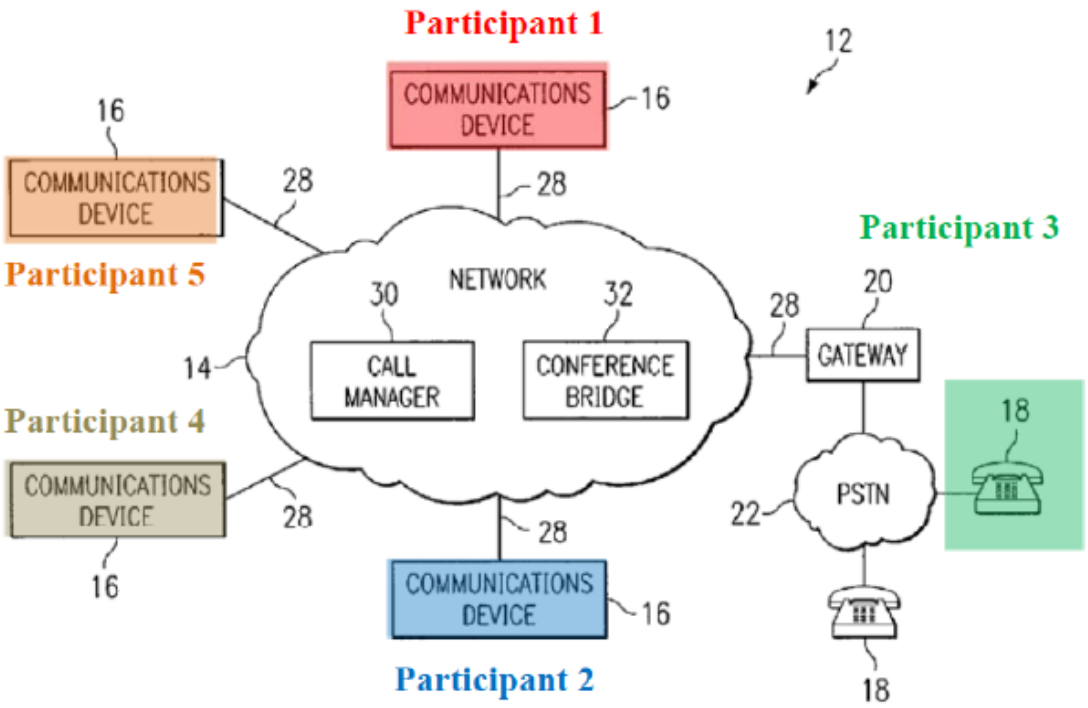
As discussed below, Patent Owner generally argues that implementing VPN tunnels with Knappe's system would not have been obvious. Patent Owner does not specifically or otherwise address Petitioner's showing regarding the preamble. *See generally* PO Resp. After a review of the record as summarized above and as discussed below in view of Patent Owner's arguments regarding the VPN tunnels and other limitations, we determine that Petitioner's showing for the preamble (even if it is limiting) based on the combined teachings of Knappe, Elliott, VPN Textbook (addressed below), and Hendricks is persuasive.

*b) Steps 19.1.1, 19.1.2, 19.2.1, and 19.2.2*

Steps 19.1.1 and 19.1.2 recite "[19.1.1] receiving first audio data, first video data, and first collaboration data at a server from a first remote client" "[19.1.2] through a first Virtual Private Network (VPN) tunnel." Petitioner relies on the combined teachings of Knapp and Elliott to address step 19.1.1 and Knapp, Elliott, and VPN Textbook to address limitation 19.1.2. Pet. 30–40. Steps 19.2.1 and 19.2.2 recite "[19.2.1] receiving second audio data at the server from a second remote client" "[19.2.2] through a second VPN

tunnel." Petitioner relies on Knapp to address step 19.2.1 and Knapp, Elliott, and VPN Textbook to address limitation 19.2.2. *Id.* at 40–44.

Petitioner annotates Knappe's Figure 1 to illustrate its showing, as follows (Pet. 34):

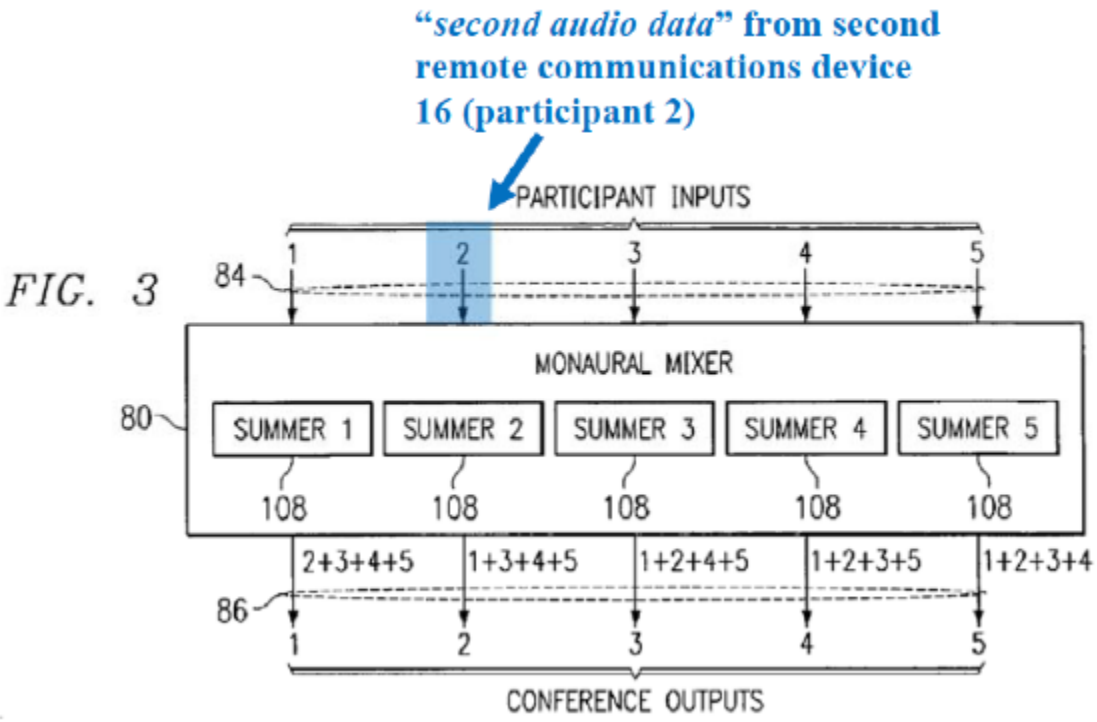



Annotating Knappe's Figure 1 above and designating participant 1 and participant 2 as red and blue communications devices 16, respectively, Petitioner reads the claimed "first remote client" of limitation 19.1.1 and "second remote client" of step 19.2.1 onto Knappe's red and blue communication devices 16, respectively. Pet. 34, 41. Petitioner contends that Knappe's "call manager 30 and conference bridge 32 provide a conferencing service where [remote] 'participants are connected and stream media through the conference bridge 32.'" *Id.* at 30 (quoting Ex. 1006, 5:31–44; citing Ex. 1003 ¶¶ 393–394).

To further support its showing, Petitioner points out that "Knappe's conference call manager 30 provides 'multiparty communications and/or other suitable services for the communications devices 16,'" and "conference bridge 32 'provides conference call and other suitable audio, video, and/or real-time multiparty communication sessions between communication devices 16.'" Pet. 30 (quoting Ex. 1006, 4:50–54, 4:58–61; citing Ex. 1003 ¶¶ 393–394). Based on these teachings and related teachings describing Knappe's Figure 1, Petitioner reads the claimed "*server*" onto "Knappe's call manager 30, either alone or in combination with the conference bridge 32, . . . because it (and they collectively) provide a conference call service to communication devices 16 and PSTN telephones 18." *Id.* at 30–31 (citing Ex. 1003 ¶ 395); *see also id.* at 44 ("[C]onference bridge 32, either alone or together with conference call manager 30, corresponds to the claimed '*server*.'").

Petitioner also relies on Knappe's teaching that mixer 80 receives and processes inputs from participants at remote devices 16. *See* Pet. 32–34, 41–43, Ex. 1006, Fig. 1, Fig. 2. Petitioner explains that Knappe's mixer 80 is part of conference bridge 32 (i.e., part of the claimed "server"). *Id.* at 32 (citing Ex. 1006, 1:29–41; Ex. 1003 ¶¶ 398–400).

For example, regarding limitation 19.2.1, "receiving second audio data at the server from a second remote client," Petitioner reproduces and annotates Knappe's Figure 3, as follows (Pet. 42):




Petitioner explains that in Figure 3, "Knappe's mixer 80 receives input audio from participant 2 [(blue)], which corresponds to the second remote communications device 16 ('*second remote client*')." Pet. 42 (citing Ex. 1006, Fig. 3; Ex. 1003 ¶¶ 426–427). Petitioner provides a similar showing for step 19.1.1. *Id.* at 34 (similarly annotating Knappe's Figs. 1 and 3 to show that step 19.1.1 reads on first audio data provided by participant 1 from first remote communication device 16).

In other words, for steps 19.1.1 and 19.2.1, Petitioner relies on Knappe's summers 1 and 2 in mixer 80 of conference bridge 32, asserting that the recited "first remote client" (participant 1) and "second remote client" (participant 2) transmits "first audio data" and "second audio data," respectively, to the claimed "server" (call manager 30 and/or conference

bridge 32, collectively). Pet. 32–34 (citing Ex. 1006, 3:62–4:16, 4:63–64, 6:59–7:11, Figs. 1, 3; Ex. 1003 ¶¶ 398–400, 402), 40–43 (citing Ex. 1006, 3:45–49, 4:58–66, 5:31–33, 6:59–7:11, Figs. 1, 3; Ex. 1003 ¶¶ 425–429).

Further regarding the "first remote client" and "second remote client" as recited in steps 19.1.1 and 19.2.1, respectively, Petitioner contends that Knappe contemplates remote clients because "Knappe's Internet transports 'packets containing data that represents audible sounds from one location to another,'" and "Knappe also refers to 'minimizing travel expenses' and how its conferencing techniques improve over 'a meeting with persons physically present in the same location.'" Pet. 31 (quoting Ex. 1006, 1:18–21, 1:42–44).

Regarding receiving "first audio data, first video data, and first collaboration data at a server from a first remote client" as limitation 19.1.1 recites, Petitioner explains that Knappe "teaches that 'conference bridge 32 receives media from participating devices 16,' which Knappe discloses as 'capable of communicating real-time audio, video, and/or other information over the network 14.'" Pet. 32 (quoting Ex. 1006, 4:63–64, 3:62–41). Petitioner similarly asserts that "Knappe teaches that '[d]uring the multiparty communications sessions, participants are connected and stream media through the conference bridge 32,' where the media includes 'audio, video, voice, data and other suitable types of real-time . . . traffic between source and destination endpoints.'" *Id.* at 36 (quoting Ex. 1006, 3:26–29, 5:31–33. Therefore, Petitioner asserts that "a POSITA would have understood Knappe's conference bridge 32 to receive 'audio, video, and/or other information' and 'data.'" *Id.* at 32 (citing Ex. 1003 ¶¶ 398–400; Ex. 1006, 1:29–41). Petitioner also asserts that "a POSITA would have understood" that Knappe's real-time traffic or media "is used for collaboration," and that

Knappe teaches "*receiving first audio data, first video data,* and first collaboration data" (*id.* at 35) from a first remote device (or from each of, or any of, Knappe's participants) (*id.* at 35–37).

Further regarding the claimed "collaboration data" as recited in limitation 19.1.1, Petitioner asserts that "a POSITA would have understood that Knappe contemplated that the real-time 'data' transmitted during conferencing . . . include well-known collaboration data, such as T.120 standard data." Pet. 35 (citing Ex. 1006, 3:27–29, 3:62–4:1, 5:45–48; Ex. 1003 ¶ 405). To supplement this assertion, Petitioner also asserts that "Elliott describes '[m]ulti-media collaboration services' allowing for the 'exchange [of] information in a conference setting.'" *Id.* (quoting Ex. 1007, 1:40–44). Petitioner further asserts that "Elliott explains such services 'include collaborative Web browsing, audio conferencing, video conferencing, and application sharing' using 'communication and application protocols' defined in the 'T.120 standard.'" *Id.* (quoting Ex. 1007, 1:40–44, 6:46–54, 5:49–61). In other words, according to Petitioner, "Elliott's teaching of collaboration services, which exchange data using the T.120 standard, discloses a multimedia conferencing stream including '*collaboration data*.'" *Id.* (citing Ex. 1003 ¶¶ 254–255, 406–407).

Noting that Knappe's communication devices 16 include personal computers (Ex. 1006, 3:62–4:1), Petitioner contends that "it would have been obvious to a POSITA that Knappe's 'other information' would include collaboration data as Elliott teaches (e.g., application sharing data, web browsing data, and other collaboration data per the T.120 standard)." Pet. 35–36 (citing Ex. 1006, 3:27–29, 3:62–4:1, 5:45–48; Ex. 1007, 1:40–44, 6:46–54, 5:49–61; Ex. 1003 ¶ 408). Petitioner explains that "[i]ncluding Elliott's collaboration data in the additional data exchanged by Knappe's

communication devices would allow different ways for the participants to collaborate thereby enhancing the effectiveness of the collaboration among the participants." *Id.* at 36 (citing Ex. 1003 ¶¶ 342–361, 408).

Summarizing with respect to step 19.1.1, Petitioner contends as follows:

> Knappe teaches that "[d]uring the multiparty communications sessions, participants are connected and stream media through the conference bridge 32," where the media includes "audio, video, voice, data and other suitable types of real-time . . . traffic between source and destination endpoints." Ex_1006, 3:26–29, 5:31–33. Accordingly, it would have been obvious to a POSITA that in the combination, conference bridge 32 would receive the audio, video, and data (such as collaboration data per Elliott) from each participant and distribute the mixed data (including audio, video, and collaboration data) to each participant. Ex_1003 ¶409. Thus, the prior art teaches that that call manager 30 and conference bridge 32 provide conference services, including receiving audio, video, and data (e.g., collaboration data such as web browsing data, application sharing data, and other collaboration data) from a first remote communications device 16, which renders this limitation obvious. *Id.* ¶410.

Pet. 36–37. This summary, which refers to "each participant" in Knappe, also applies to the recited "second audio data" and "second remote client" (Knappe's participant 2) in limitation 19.2.1, as Petitioner relies partly on its showing for limitation 19.1.1 to address 19.2.1. *See id.* at 40–43.

In response, Patent Owner contends that the combined teachings of Knappe and Elliott do not teach limitation 19.1.1, "receiving first audio data, first video data, and first collaboration data at a server from a first remote client." PO Resp. 19–20. However, as Petitioner notes, Patent Owner does not specify what aspect of limitation 19.1.1 is missing from the combined teachings of Knappe and Elliott. *See id.*; Reply 10.

Rather, Patent Owner alleges that based on "fundamental difference[s]" between Elliott's and Knappe's system, "Elliot lacks the motivation to be integrated with Knappe." PO Resp. 20 (citing Ex. 2001 ¶¶ 18–19). According to Patent Owner, "Elliott simply discloses two independent calls with two independent remote parties connected to a call-center," and "[t]he system is not subject to modification with the other references, including Knappe." *Id.* at 19–20. In its Sur-reply, Patent Owner builds on this argument and points to teachings in Elliott involving an agent and argues that "[g]iven Elliott's *teaching away* of sharing audio data between remote parties, it would not be combined with Knappe which does involve sharing audio and video between remote parties." Sur-reply 8 (emphasis added). Patent Owner also argues that "Knappe/Elliott also do not disclose collaboration data as a distinct set of data from video and audio." *Id.*; *accord* PO Resp. 31 (presenting similar arguments).

These arguments are unavailing. The Petition relies on the combined teachings of the references, and Patent Owner's arguments attack specific aspects of Elliott's agent/call center embodiment (a preferred embodiment), instead of addressing Petitioner's reliance on the combined teachings of the references (i.e., Knappe, Elliott and the VPN Textbook), including Elliott's general teachings regarding Figure 1's Internet network 18, and also its general disclosures of multi-party conferencing, collaboration data, and VPN tunnel teachings, which broadly apply to Internet 18. *See* Pet. 12–24, Sur-reply 5–9; Ex. 1007, 8:13–40.

Contrary to Patent Owner's teaching away arguments, as summarized above, Elliott specifically teaches providing audio and therefore does not teach away from providing audio between remote parties. Moreover, Patent Owner otherwise admits that Elliott discloses "secure audio data." PO

Resp. 29. As indicated, the Petition specifically shows that Elliott teaches transmitting audio. For example, the Petition persuasively shows that Elliott discloses "collaborative Web browsing, *audio conferencing*, video conferencing, and application sharing." Pet. 35 (emphasis added) (quoting Ex. 1007, 1:43–44; citing Ex. 1003 ¶ 346); *accord* Reply 12 (same showing) (quoting Ex. 1007, 1:43–44; citing Ex. 1003 ¶ 346). The Petition similarly shows that Elliott discloses "connecting calls 'over the public switched telephone network (PSTN) 30' using 'session server 12 . . . that follows the ITU T.120 standard' capable of 'support[ing] real-time, multi-point data communications,' the server 'able to set up to conduct video conferences, *audio conferences*, and data conferences with application sharing,' as well as '[c]ollaborative Web browsing.'" Pet. 18 (alteration in original) (quoting Ex. 1007, 5:35–61; Ex. 1003 ¶¶ 346–347); *accord* Reply 12–13 (same showing) (quoting Ex. 1007, 5:35–61; citing Ex. 1003 ¶¶ 346–347). And as summarized above, Petitioner shows that both Knappe and Eliott disclose different types of collaboration data per the T.120 standard, including application sharing data, web browsing data, and other collaboration data. *See* Pet. 35–36 (citing Ex. 1006, 3:27–29, 3:62–4:1, 5:45–48; Ex. 1007, 1:40–44, 6:46–54, 5:49–61; Ex. 1003 ¶ 408).

Accordingly, based on the foregoing as summarized above, both Elliott and Knappe disclose collaborative web browsing with audio and video as distinct types of data, contrary to Patent Owner's arguments and related argument that the references are not similar. Moreover, Patent Owner admits that "Elliot . . . enables multimedia collaboration." PO Resp. 22.

In addition, as outlined above, the Petition relies on Elliott's Figure 1 and its network 18, which includes the transfer of packet data over the

Internet, similar to Knappe's system. *See, e.g.*, Pet. 17 (citing Ex. 1007, 5:35–39 (discussing client computer 20, depicted in Fig. 1 ), 6:1–11 (discussing web server 14 and "packetswitched IP network 18," depicted in Fig. 1), Fig. 1; Ex. 1003 ¶ 343), 31 (noting Knappe's transfer of packets containing audio data over the Internet). With further respect to Elliott's network 18, Elliott specifically states that "[t]he present invention provides a method and system *for communications between remote parties*. Parties are considered to be remote from each other when they are separated by a network 18." Ex. 1007, 3:64–67 (emphasis added). That is, contrary to Patent Owner's arguments, as Petitioner shows, Elliott's network 18, like that of Knappe, supports all manner of communications between remote parties, including via audio IP packets. *See* Reply 11 ("Elliott explicitly states that its system 'also enables services for one-to-many and many-to-many IP based collaboration[.]'" (quoting Ex. 1007, 2:10–13; citing *id.* at 7:58–61 (discussing "multiple 1:1, 1:n, n:1, and n:n sessions")).

In general, then, as summarized above (§ III.D.2), Elliott is similar to Knappe and generally discloses "multi-media collaboration . . . among multiple parties." Ex. 1007, 2:58–60. "Multi-media collaboration refers to the use of more than one media stream (e.g.: voice, fax, data, video, etc.) used in collaboration with *more than one party*." *Id.* at 2:66–3:1 (emphasis added). Some "examples of multi-media collaboration" include "*multi-party conferencing*," and "virtual private networks." *Id.* at 3:1–6 (emphasis added). Elliott's "system and method of the present invention can also enable services for one-to-many and many-to-many IP-based collaboration." *Id.* at 3:13–15.

Based on teachings in the references, Petition contends that it would have been obvious to implement Elliott's collaboration data (and VPN

tunnel teachings as discussed below) with Knappe's system for numerous reasons supported by the record as summarized above. *See* Pet. 35–37; Reply 10–13. For example, summarizing the Petition's showing, Petitioner contends that "[i]t would have been obvious to a POSITA, in view of Elliott's teachings, to implement Knappe's transmission of various types of data as collaboration data, because this type of collaboration data would allow a greater variety of information among the participants, improving the experience and enhancing the effectiveness of collaboration in a variety of contexts." Reply 13 (citing Ex. 1003 ¶ 348); *see also* Pet. 35–36 (similar showing (citing Ex. 1006, 3:26–29; 5:31–33; Ex. 1003 ¶¶ 342–361, 409)). Therefore, Petitioner also provides articulated rationale with factual underpinnings to show persuasively that it would have been obvious to employ distinct collaboration data (distinct from audio and video data) in Knappe's system based on the combined teachings of Knappe and Elliott to supplement the audio and video data during a conference.

Based on the summary outlined above, Petitioner also shows persuasively that this collaboration data would have improved Knappe's similar conferencing system, summarizing as follows:

> [T]he combination of Knappe and Elliott is merely the ordinary use of common techniques (transmitting collaboration web browsing data, application sharing data, and collaboration data per the T.120 standard as Elliott teaches) to improve the similar conferencing system of Knappe in the same way by allowing for enhanced collaboration among participants.

Reply 14 (citing Ex. 1003 ¶ 352).

Based on the record and foregoing discussion, we find that Petitioner articulates persuasive rationale supported by the record to show that the combined teachings of Knappe and Elliott satisfy steps 19.1.1 and 19.2.1.

Regarding the VPN tunnel recitations of step 19.1.1 ("receiving first audio data, first video data, and first collaboration data at a server from a first remote client" "[19.1.2] through a first Virtual Private Network (VPN) tunnel") and similar step 19.2.1 ("receiving second audio data at the server from a second remote client" "[19.2.2] through a second VPN tunnel"), Petitioner annotates VPN Textbook's Figure 7-10, as follows (Pet. 43):

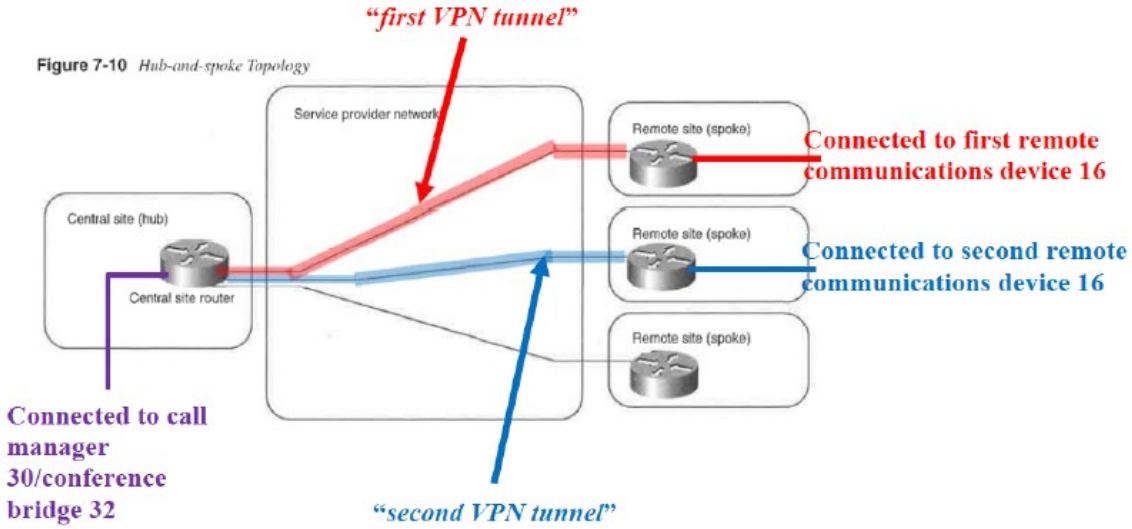



Figure 7-10 as annotated by Petitioner illustrates a first VPN tunnel (red) and a second VPN tunnel (blue). Based on the combined VPN teachings of Knappe, Elliott, and VPN Textbook, Petitioner shows the VPN tunnels connected in a typical "*Hub-and-spoke Topology*" (Ex. 1010, 129, Fig. 7-10), with Knappe's call manager and conference bridge 32 (purple) at the central hub router, and Knappe's first and second remote communication devices 16 (red, blue), connected at the remote ends of the spokes through routers located there. *See* Pet. 37–40 (citing Ex. 1010, 129, Fig. 7; Ex. 1006, 4:30–33, Fig. 1; Ex. 1003 ¶¶ 419–421), 43–44 (citing Ex. 1010, Fig. 7; Ex. 1003 ¶¶ 430–434).

Petitioner contends that using VPN connections as Elliott and VPN Textbook suggest would have been obvious because VPNs provide "secure

communications among the connected devices in a cost effective and relatively simple way." Pet. 44 (citing Ex. 1003 ¶¶ 342–370, 433). To support its showing, as indicated above in annotated Fig. 7-10, Petitioner points to similarities between Knappe's topology and VPN Textbook's hub-and-spoke technology, including Knappe's centrally located call manager 30 and conference bridge 32 (like a hub) connected to remote devices 16 (like spokes). *See id.* at 38–39 (citing Ex. 1006, 1:42–47, 3:62–4:1, 4:30–31, 6:17–21, Fig. 1; Ex. 1010, Fig. 7-10, 129–30; Ex. 1003 ¶ 419).

Petitioner also relies on Elliott's above-discussed teaching of "multi-media collaboration," including "voice, fax, data, video" transmitted over a "virtual private network (VPN)" using "IP or IP-tunneling." Pet. 37 (quoting Ex. 1007, 2:66–67, 4:31–33; citing Ex. 1003 ¶¶ 234–235, 413). According to Petitioner, based on Elliott's VPN and IP-tunnel teachings, "it would have been obvious to a POSITA to utilize VPN tunneling when communicating audio, video, and collaboration data between the first remote communication devices 16 and the call manager 30/conference bridge 32, because it would provide Knappe with secure communications as the communications traverse the Internet network 14." *Id.* (citing Ex. 1003 ¶¶ 234–235, 414).

Petitioner also relies on VPN Textbook's teachings that describe the hub-and-spoke VPN topology as cost effective and simple, as follows:

> A POSITA would have understood that each remote site router (spoke) would have one or more network devices connected to it. Ex_1003 ¶¶416–417. As explained above, Knappe's devices may be at different remote locations on the network. *See, e.g.*, discussion at [19.1.1]; Ex_1006, 4:30–33, FIG. 1. Thus, when implementing VPN tunneling in Knappe, per Elliott, it would have been obvious to a POSITA to connect each of Knappe's devices (which are located at different locations) to

> a separate remote router (spoke) that is connected to the central router (hub), as the VPN Textbook teaches, because this common topology provides a cost effective and less complex implementation. Ex_1003 ¶418; Ex_1010 at 129 ("has nonetheless chosen the hub-and-spoke topology for cost or complexity reasons."); *see also* Ex_1003 ¶¶ 362–370.

Pet. 38.

Focusing on the VPN Textbook, Patent Owner contends that "the USPTO has already determined that general VPN textbooks are not invalidating prior art, having considered during prosecution [three VPN textbooks]." PO Resp. 14. Patent Owner reasons "[t]his is so because the principal references disclose nothing about how to implement a VPN or VPN tunnel in a web videoconferencing network." *Id.* at 15.

Patent Owner's arguments do not undermine Petitioner's showing because Petitioner does not rely on the VPN Textbook alone, and the record shows that artisans of ordinary skill knew how to implement a VPN tunnel in a web videoconferencing scheme as indicated in the summary above and as discussed further below. For example, and as outlined above, Elliott discloses use of a VPN tunnel in a web conferencing scheme. Petitioner specifically relies on Elliott's teaching of "multi-media collaboration," including "voice, fax, data, video" transmitted over a "virtual private network (VPN)" using "IP or IP-tunneling." Pet. 37 (quoting Ex. 1007, 2:66–67, 4:31–33; citing Ex. 1003 ¶¶ 234–235, 413). Moreover, Petitioner persuasively shows that the VPN Textbook teaches that a hub-and-spoke VPN topology was a known security option chosen for cost effectiveness and complexity reasons, and Knappe's system is in a hub-and-spoke topology. *See* Pet. 37-38 (citing Ex. 1003 ¶¶ 418, 362–370; Ex. 1010, 129 (noting "[t]he most commonly encountered topology is a hub-and-spoke

topology," "the hub-and-spoke VPN topology is more common than you might expect," and "there are many examples where the customer could benefit from a different topology but has nonetheless chosen the hub-and-spoke topology for cost or complexity reasons")).

Nevertheless, Patent Owner also argues that the first and second VPN tunnel limitation would not have been obvious. *See* PO Resp. 26–27. Patent Owner contends that "Petitioner has broken the complete claim element into two parts. The element is 'receiving first audio data, first video data, and first collaboration data at a server from a first remote client through a first Virtual Private Network (VPN) tunnel.'" PO Resp. 21. These arguments are unavailing. As discussed above and below, Petitioner relies on the combined teachings of the references to address the "two parts" of the claim steps (i.e., 1) types of packets in 2) a VPN tunnel).

Patent Owner argues that "to show the presence of the VPN tunnel, Petitioner has combined Elliot (EX_1007) with Knappe or Drell." PO Resp. 21. Patent Owner also contends that "Elliot teaches combining a traditional analog phone connection with an agent workstation," but that

> [n]either of the two disparate parts of [Elliot's] invention—a one-to-one POTS [(plain old telephone system)] or PSTN phone connection—would suggest to a person or ordinary skill in the art that a VPN should or could be implemented to protect voice over the Elliott POTS phone connection or access to a publicly-available URL on the Web.

PO Resp. 21–22 (citing Ex. 2001 ¶ 21). Patent Owner also contends that a VPN "cannot be implemented over PSTN." *Id.* (citing Ex. 2001¶¶ 21–22).

Tracking its unavailing arguments addressed above regarding collaboration data, Patent Owner also argues that Elliott's system "enables multimedia collaboration" by "establishing separate sessions for each party,"

to allow "two independent calls with two independent remote parties connected to a call-center." PO Resp. 22. According to Patent Owner, "the discussion in Elliott related to VPNs is never in relation to mixed audio as claimed." *Id.* at 21–22 (citing Ex. 2001 ¶ 23). Patent Owner similarly argues as follows:

> The limitation regarding provision of a VPN tunnel to protect ***mixed audio*** is taught by neither [Knappe nor Elliott]. Although Elliott mentions in passing a Virtual Private Network (VPN), its application can only be understood as directed to "network **18**," which is used to connect two computers over the Internet, and not audio data, mixed or otherwise.

PO Resp. 23 (quoting Ex. 1007, 4:6–19).

These arguments address limited teachings in Elliott in isolation and fail to address Petitioner's persuasive reliance on the teachings of Knappe, Elliott, and the VPN Textbook, as supplemented by the knowledge of an artisan of ordinary skill. *See* Reply 14 ("Patent Owner's arguments fail to address anything other than Knappe and Elliot," where "for the VPN tunneling limitations," "Petitioners rely on Knappe in combination with Elliot and *the VPN Textbook* as viewed by one skilled in the art."). As also discussed above and below, Petitioner relies on Knappe for its mixed audio teachings. Petitioner does not rely on Drell specifically to address the VPN tunnel limitations.

In addition, and contrary to Patent Owner's arguments, Petitioner does not seek to employ Elliott's VPN teachings to protect voice of a POTS phone connection, access a URL on the Web, or implement VPN on a PSTN network. Moreover, the challenged claims do not require these features. Rather, Petitioner relies on Elliot's VPN teachings as applicable to multiple parties using individual private networks, even if Elliot discloses "two

independent calls" in its agent/call center embodiment. *See* PO Resp. 17. For example, as Petitioner shows and as discussed above in connection with Elliott's collaboration teachings, Elliott teaches transmitting audio data packets during multi-party conferencing, where "Elliott explicitly states that its system 'also enables services for one-to-many and many-to-many IP based collaboration.'" *See* Reply 11 (quoting Ex. 1007, 2:10–13; citing Ex. 1007, 7:58–61 (discussing "multiple 1:1, 1:n, n:1, and n:n sessions")).

Petitioner also persuasively shows that "VPN's and VPN tunneling were a known solution for securing communications over public networks." Reply 15 (citing Ex. 1003 ¶¶ 356–361). As Petitioner notes, "the VPN Textbook . . . states that 'more and more business-to-business traffic takes place over the Internet' and that this type of communication is 'riddled with security issues.'" *Id.* (quoting Ex. 1010, 119). And "Knappe's communications system transmits 'audio, video, voice, data and other suitable types of . . . traffic between source and destination endpoints' across 'network 14 [which] is the Internet.'" *Id.* (quoting Ex. 1006, 3:26–58). To secure this data over the Internet, "[a] Virtual Private Network (VPN) . . . [provides] connectivity amongst multiple sites . . . with the same access or security policies as a private network." *Id.* (quoting Ex. 1010, 115).

As to Patent Owner's argument that that the district court construed a VPN tunnel as "a private network of securely connected appliances configured within a public network" (PO Resp. 25–26), as summarized above, Petitioner shows that the VPN tunnels securely connect the claimed server with first and second remote clients (appliances). *See* Pet. 44 (showing that VPNs provide "secure communications among the connected devices [of Knappe] in a cost effective and relatively simple way"—with connected devices including "remote communication device 16 and call

manager 30/conference bridge 32"). *Id.* (citing Ex. 1003 ¶¶ 342–370, 433). As Petitioner also argues, Elliott expressly discloses a VPN tunnel. Reply 22. To support its showing, Petitioner quotes Dr. Houh who testifies that "[t]unneling refers to a networking technique whereby a packet is encapsulated in another network packet, typically so that it can traverse an underlying network that does not support the capability required by the encapsulated packet." *Id.* (quoting Ex. 1003 ¶ 83). Patent Owner agrees that "[a] VPN tunnel . . . is construed to mean 'a connection between two devices that permits encapsulating a first packet from one protocol in a second packet from a different protocol.'" PO Resp. 25 (quoting Ex. 2002).

Therefore, the record shows that VPN tunnels were well-known to provide encrypted packets on the Internet to securely connect appliances transmitting and receiving same, which satisfies the district court claim construction. *See also* Ex. 1003 ¶ 91 ("VPNs were known to be used to securely exchange data between different locations over the Internet." (citing VPN Textbook, 118–119 (displaying "[e]ncrpyted point-to-point tunnels (IPSec)" over a "Public Internet" between different "Firewalls" at three "Organizations" as a "Typical Extranet Setup" at Fig. 7-3); Ex. 1020, 2:65–3:3, 5:52–55)); Reply 17 (citing Ex. 1020, 5:52–55 (("VPN refers to a network that is carried over public networks, but which is encrypted to make it secure from outside access and interference.").

As further evidentiary support, Petitioner provides citations to prior art patents and shows that artisans of ordinary skill readily employed VPNs to secure data over public networks including for videoconferencing systems. Reply 16 (citing Ex. 1019, 2:66–3:1, 4:23–27, 6:36–41 (describing a "conference bridge application" that transmits "data 'over public networks,

using . . . [a] Virtual Private Network (VPN)"); Ex. 1020 2:65–3:3, 5:52–55 ((disclosing "need for a videoconferencing system . . . for delivering secure . . . services over an IP network" by using a "VPN . . . over public networks . . . which is encrypted to make it secure from outside access and interference"); Ex. 1023 ¶¶ 1412, 1415–1453 (describing "VPN connectivity," including "hub-and-spoke or mixed topologies" in the context of "services [that] include Internet Access, . . . chat and Video-conferencing etc.").

Similar to these prior art patents and as summarized above, Petitioner notes that Elliott teaches utilizing a "virtual private network (VPN) . . . which uses IP or IP-tunneling" to transmit "voice, fax, data, video" and "[o]ther types of collaboration . . . data." Pet. 21 (quoting Ex. 1007, 2:66–3:1, 4:29–34, 6:53–54; citing Ex. 1003 ¶ 359). Petitioner also shows that VPN tunnels involve encryption and packet encapsulation under well-known protocols (IPsec), and Knappe discloses mixed audio and other types of data (e.g., audio, video, information) traveling in packets. *See id.* at 31–32 (citing Ex. 1006, 1:18–41, 4:63–64, 3:62–4:1, 6:59–7:11); Ex. 1010, 117–119; Ex. 1003 ¶¶ 76–88 (noting that Internet Protocol (IP) involves packets, and describing, *inter alia*, IPSec, tunneling, and other standard packet protocols). Supporting Petitioner, Dr. Houh testifies that "Elliott utilizes VPN tunneling for communicating conferencing voice, video, and collaboration data over a public network 18, such as the Internet." Ex. 1003 ¶¶ 236, 234–235 (citing Ex. 1007, 2:66–3:1, 4:31–34; 6:53–54). Similar to Knapp's Internet network 14, Elliott's Internet network 18, which Petitioner relies upon, is a "packet switched IP network." Ex. 1007, 6:9.

Therefore, even if Elliott does not explicitly disclose mixed audio as Patent Owner argues, Petitioner shows persuasively that it would have been

obvious to provide VPN tunnels for Knapp's mixed audio and other packet data by encrypting and then encapsulating the packet data in a well-known manner. As Petitioner also shows, the mixed audio and other packets emanating from Knappe's participants travel to one destination (a particular participant) at each output of mixer 80. *See, e.g.*, Ex. 1006, 7:1–2 ("During normal operation, each participant receives the audio input of each other participant. Thus, for example, the conference output stream of participant 1 includes the audio inputs of participants 2–5."), Fig. 3. Therefore, providing a VPN tunnel by encrypting and encapsulating a mixed stream of packets involves materially the same process as that for non-mixed packet streams, because in both cases, the packet streams travel to a single destination. In any case, as summarized above, Petitioner articulates persuasive rationale with a reasonable expectation of success to implement VPN tunnels for mixed audio data and other data as claimed.

For example, based on "Elliott's VPN and VPN Textbook's teachings," Petitioner contends that "it would have been obvious to . . . utilize VPN tunneling when communicating audio, video, and collaboration data across Knappe's Internet network 14 because VPN tunneling would make the transmitted data secure from outside access and interference." Reply 16–17 (citing Ex. 1003 ¶¶ 356–361; Ex. 1020, 5:52–55 ("VPN refers to a network that is carried over public networks, but which is encrypted to make it secure from outside access and interference.").

Moreover, Petitioner shows that artisans of ordinary skill would have known that "VPNs are beneficial because they reduce the need to lease private data lines, which reduces or avoids the costs for implementing a private network by communicating securely over the Internet." Reply 17 (citing Ex. 1026, 44:10–12 ("[O]ffices [] create virtual private networks

(VPNs) to save money on remote access and interoffice connectivity."). Therefore, notwithstanding Patent Owner's arguments, Petitioner shows persuasively that it would have been obvious to employ a VPN tunnel for packets traveling over the Internet as a well-known solution to secure Knappe's Internet conferencing data (e.g., as supplemented by Elliott's collaboration data teachings), where the VPN Textbook shows that it was known that the Internet is not secure, with traffic "vulnerable to eavesdropping and other problems." *Id.* at 15. In other words, as Petitioner argues, "[t]he VPN Textbook is used in combination with the[] references in each of the three grounds . . . show that the alleged invention is no more than 'a combination of familiar elements according to known methods . . . [that] does no more than yield predictable results.'" *Id.* at 4 (bracketed alterations in original) (quoting *KSR*, 550 U.S. at 401)).

After a review of the record as summarized above, we determine that Petitioner's showing for steps/limitations 19.1.1, 19.1.2, 19.2.1, and 19.2.2 based on the combined teachings of Knapp, Elliott and VPN Textbook is persuasive.

*c) Limitation 19.3*

Limitation 19.3 recites "receiving third audio data at the server from a Public Switched Telephone Network (PSTN) client through a PSTN gateway." Petitioner relies on Knappe's "teach[ing] that 'telephones 18 communicate standard telephony signals through PSTN 22 to the gateway 20.'" Pet. 44 (quoting Ex. 1006, 4:18–20). Petitioner quotes Knappe as teaching that "[a]t the gateway 20, the signals are converted to IP packets in the VoIP format." *Id.* (quoting Ex. 1006, 4:20–22). Then, "[c]onference bridge 32 . . . 'receives media from participating devices 16.'" *Id.* 44-45 (quoting Ex. 1006, 4:63–66).

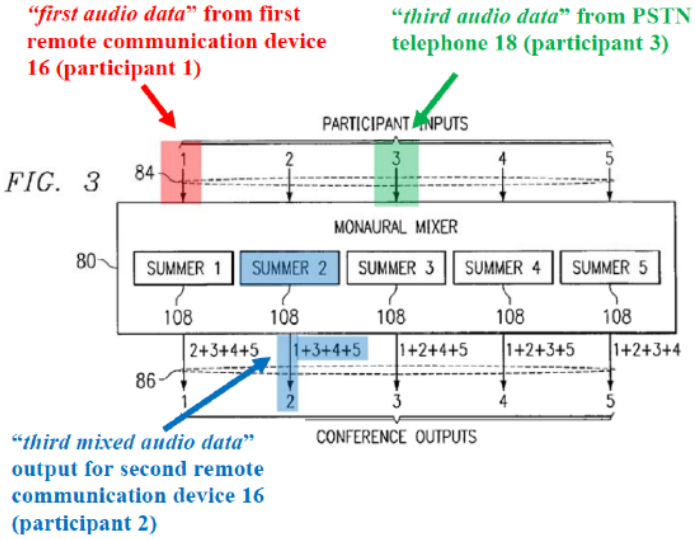
Based on these PSTN teachings, Petitioner contends that "a POSITA would have understood that when the PSTN telephone 18 is the originating device, it sends data over gateway 20 which communicates the data to the conference bridge 32, which facilitates the multiparty communications." Pet. 45 (citing Ex. 1003 ¶¶ 437–438). In other words, Petitioner reads the recited "third audio data" onto data from PSTN telephone 18. Petitioner further relies on Knappe's mixer 80 of conference bridge 32 (i.e., at the claimed server) as receiving "third audio data" from participant 3 at PSTN telephone 18. *See id.* at 45–56 (citing Ex. 1003 ¶¶ 439, 441–442; Ex. 1006, Fig. 1, Fig. 3).

After a review of the record as summarized above, we determine that Petitioner's showing for limitation 19.3 based on Knappe is persuasive. Patent Owner does not specifically address Petitioner's showing as to this step. *See generally* PO Resp.

*d) Steps 19.4–19.9*

Steps 19.4–19.9 generally recite mixing the audio data of steps 19.1.1, 19.2.1, and 19.3 from two of the clients and transmitting it to another client. Specifically, step 19.4 recites "mixing the first audio data with the second audio data into a first mixed audio data" and step 19.7 recites "transmitting the first mixed audio data from the server to the PSTN client through the PSTN gateway." Step 19.5 recites "mixing the second audio data with the third audio data into a second mixed audio data" and step 19.8 recites "transmitting the second mixed audio data from the server to the first remote client through the first VPN tunnel." Step 19.6 recites "mixing the first audio data with the third audio data into a third mixed audio data," and step 19.9 recites "transmitting the third mixed audio data from the server to the second remote client through the second VPN tunnel."

Petitioner relies on Knappe's mixer 80 to illustrate how Knappe's server performs mixing and transmitting as steps 19.4–19.9 require. For example, for steps 19.6 and 19.9, Petitioner annotates Knappe's Figure 3 as follows (Pet. 50, 56):




As annotated by Petitioner, Knappe's Figure 3 illustrates mixing "first audio data" from participant 1 at first remote communication device 16 (red) with "third audio data" from participant 3 and PSTN telephone 18 (green) at mixer 80's summer 2 (blue) to create "third mixed audio data" for transmitting to participant 2 at "second remote client" communication device 16 (blue), as steps 19.6 and 19.9 require. Pet. 50, 56 (citing Ex. 1006, 3:24–29, 5:31–39, 7:1–7, 4:42–51 ("each device 16 receives a conference signal that includes contributions from all other participating devices"), Fig. 3; Ex. 1003 ¶¶ 472–474).

Addressing the VPN tunnel limitation, Petitioner explains that "[w]hen the conference bridge 32 transmits the third mixed audio data to the second remote communications device 16, the data would be sent through the second VPN tunnel that was already established (see discussion at [19.2.2]), which corresponds to '*the second VPN tunnel.*'" *Id.* at 57 (citing

Ex. 1003 ¶¶ 475–476). Similar to its VPN assertions discussed above, Petitioner contends that using the established second VPN tunnel would have been obvious in view of the VPN Textbook and Elliott for transmitting the third mixed audio data because the tunnel would "secure" the data in "a cost effective and relatively simple implementation." *Id.* at 56–57 (citing Ex. 1003 ¶¶ 475–477).

Petitioner applies a similar analysis for the other of the two claimed clients. That is, for step 19.7's "transmitting the first mixed audio data . . . to the PSTN client," Petitioner refers back to its showing for limitation 19.4, wherein Knappe teaches generating "*first mixed audio data*" of summer 3 as an output intended for participant 3 using the PSTN telephone, and then annotates Knappe's Figure 1 to show how Knappe teaches transmitting "first mixed audio data" from the server to participant 3 at the "PSTN client" and "PSTN gateway" as limitation 19.7 requires. Pet. 46–47 (addressing "mixing" step 19.4's "first mixed audio data"), 51–52 (addressing "transmitting" step 19.7).

Similarly, for step 19.8's "transmitting the second mixed audio data . . . to the first remote client," Petitioner refers back to its showing for limitation 19.5, wherein Knappe teaches generating "second mixed audio data" as an output from the server to Knappe's participant 1 at communication device 16, "the first remote client." *See* Pet. 48–49, 52 (addressing "mixing" step 19.5's "second mixed audio data"), 53 (annotating Ex. 1006, Fig. 3 and addressing "transmitting" step 19.8). Petitioner further shows how the combined teaching of Knappe, the VPN Textbook, and Elliott teach transmitting this second mixed audio data through the first VPN tunnel to the first communication device as limitation 19.8 requires. *See id.* at 53–55.

After repeating steps 19.4–19.9 (PO Resp. 17–18), Patent Owner argues that the prior art does not disclose "this sequence of mixed audio signals" (*id.* at 19). According to Patent Owner, "Drell simply says a single mixer combines 'in the broadest and most general sense,'" and "Knappe says that mixing can be a 'suitable mix dictated by the type of multiparty session and/or the participant.'" *Id.* (quoting Ex. 1008, 5:8–2; Ex. 1006, 5:33–39). According further to Patent Owner, "[n]either Drell nor Knappe reflect or disclose an understanding of the requirements of the different mixers or would teach or suggest this to a person of skill in the art." *Id.* (citing Ex. 2001 ¶ 20). Patent Owner focuses on step 19.6 and relies on its unavailing arguments regarding the VPN tunnel limitations addressed above. PO Resp. 29–30.

These arguments are unavailing. Petitioner does not rely on Drell for these claim limitations. Also, the challenged claims do not require "different mixers." In short, with the exception of the above-discussed VPN tunnel limitations, Patent Owner fails to address Petitioner's showing. As summarized above, Petitioner persuasively shows that Knappe discloses multiple summers in mixer 80 (thereby operating as separate mixers even if claim 19 requires that somehow) and shows how steps 19.4–19.9 read on the combination, including the recited mixing of first, second, and third audio data to obtain the "first mixed audio data," "second mixed audio data," and "third mixed audio data" of steps 19.4–19.6, according to any "sequence" dictated by the steps. Pet. 46–51. Petitioner also persuasively shows that Knappe discloses "transmitting" the first, second and third, "mixed audio data" according to steps 19.7–19.9. *Id.* at 51–57. Petitioner persuasively essentially repeats and summarizes this analysis in its Reply, specifically showing (again) how summers 1–3 of mixer 80 create first, second, and third

mixed audio data at Knappe's conference outputs for transmission to the recited clients according to steps 19.4–19.9. Reply 5–10 (annotating Ex. 1006, Figs. 1 and 3 and reading claim steps thereon).

In summary, Petitioner shows persuasively that, just like the claim steps, Knappe's mixer simply mixes audio data from a plurality of participants (e.g., 1, 3, 4, 5) and transmits that mixed audio data as a conference output to a participant (e.g., 2) that is not one of the plurality (e.g., 1, 3, 4, 5), performing the recited mixing and transmitting via outputs from summers 1–5 for each of five participants (where claim 19 only requires transmission to three clients). *See, e.g.*, Pet. 56 (annotating Ex. 1006, Fig. 3).

Relying on Knappe's mixing, summer, conference participants (which include a PSTN participant), the VPN Textbook, and Elliott, as summarized above, Petitioner provides persuasive rationale supported by factual underpinnings of record to show the obviousness of steps 19.4–19.9. *See* Pet. 46–57. Other than its above-discussed arguments related to the VPN tunnel limitations, and its above-discussed generic arguments regarding separate mixers and other unclaimed limitations, Patent Owner does not specifically address Petitioner's persuasive showing and rationale related to steps 19.4–19.9.

After a review of the record as summarized above, we determine that Petitioner's showing for steps 19.4–19.9 based on the combined teachings of Knappe, VPN Textbook, and Elliott is persuasive.

*e) Step 19.10*

Step 19.10 recites "transmitting the first video data and the first collaboration data from the se[r]ver to the second remote client." Referring to its showing for step 19.1.1, Petitioner contends that the claimed server

reads on Knappe's conference bridge 32 and/or conference call manager 30 and that "Knappe in combination with Elliott teaches that the conference bridge 32 receives the first video data and the first collaboration data from the first remote communications device 16." Pet. 58 (citing Ex. 1003 ¶ 489).

Petitioner also contends that Knappe's "conference bridge 32 transmits video data and collaboration data to the communications devices 16." Pet. 58 (citing Ex. 1006, 3:24–29 ("[T]he communication system 12 is a distributed system transmitting audio, video, voice, data and other suitable types of real-time . . . traffic.")). Similar to its showing for limitation 19.1.1, Petitioner also relies on Knappe's teaching that "[d]uring the multiparty communications sessions, participants are connected and stream media through the conference bridge 32," where the media includes "audio, video, voice, data and other suitable types of real-time . . . traffic between source and destination[ ]end[ ]points." Pet. 59 (quoting Ex. 1006, 3:26–29, 5:31–33).

Also similar to its showing for step 19.1.1, Petitioner contends that "Elliott teaches transmitting collaboration data, such as 'application sharing' data, 'web browsing' data, and data per the 'T.120 standard.'" Pet. 58–59 (quoting Ex. 1007, 1:43–44, 6:52, 5:49–50; citing Ex. 1003 ¶¶ 254, 289, 406, 483; Ex. 1007, 1:40–44; 5:49–61, 6:46–54). Based on the teachings in Knappe and Elliott, Petitioner contends that implementing Knappe's communication devices 16 in the form of Knappe's personal computers as Knappe teaches, suggests using Elliott's web browsing and application data with video in view of Knappe's teaching of streaming different types of data or media through the conference bridge for multi-party communications, where the "output stream for a participant includes the media of all other participants." *Id.* (quoting Ex. 1006, 5:35–39; citing Ex. 1003 ¶¶ 482, 484).

According to Petitioner, "[i]ncluding Elliott's collaboration data in the additional data exchange by Knappe's communication devices would allow different ways for the participants to collaborate thereby enhancing the effectiveness of the collaboration among the participants," including for a participant at the remote second communications device 16. *Id.* at 59 (citing Ex. 1003 ¶¶ 342–361, 484).

Patent Owner relies on its above-discussed unavailing arguments that Elliott teaches away from audio, Elliott and Knappe include fundamental differences, and "neither Knappe nor Elliot disclose collaboration data as a distinct set of data from video and audio." PO Resp. 31.

After a review of the record as summarized above, we determine that Petitioner's showing for step 19.10 based on the teachings of Knappe and Elliott is persuasive. Patent Owner does not address limitation 19.10 separately. We address Patent Owner's unavailing arguments related to the collaboration data above.

*f) Summary*

As summarized above, the record supports Petitioner's obviousness showing, including reasons supported by factual underpinnings of record to combine the reference teachings with a reasonable expectation of success. Accordingly, we determine that Petitioner shows by a preponderance of evidence that claim 19 would have been obvious over Knappe, Elliott, VPN Textbook, and Hendricks.

*6. Dependent claims 20, 21, and 25–27*

Claims 20 and 21 depend directly from independent claim 19, and claims 26 and 27 depend directly from independent claim 25. Independent claim 25, an apparatus claim, is materially similar to claim 19, a method claim. Petitioner contends that these claims would have been obvious under

35 U.S.C. § 103(a) based on the combined teachings Knappe, Elliott, VPN Textbook, and Hendricks. *See* Pet. 60–62. In support, Petitioner relies on the testimony of Dr. Houh and provides citations to the reference teachings. *Id.* Petitioner persuasively maps the steps and/or limitations of claims 20, 21, and 25–27 to the asserted prior art and provides reasons supported by factual underpinnings of record to combine the reference teachings with a reasonable expectation of success. *See id.*

Patent Owner groups claims 19 and 25 together, relying material the same unavailing arguments addressed above in connection with claim 19. *See* PO Resp. 16–19.

Based on the foregoing discussion and record, we determine that Petitioner shows by a preponderance of evidence that claims 20, 21, and 25–27 would have been obvious based on the combined teachings of Knappe, Elliott, VPN Textbook, and Hendricks.

*E. Obviousness, Claims 22–24, 28, and 29*

Claims 22–24 depend directly or indirectly from independent claim 19, and claims 28 and 29 depend directly or indirectly from independent claim 25. As noted above, independent claim 25, an apparatus claim, is materially similar to claim 19, a method claim. Petitioner contends that these claims would have been obvious under 35 U.S.C. § 103(a) based on the combined teachings Knappe, Elliott, VPN Textbook, Hendricks, and Drell. *See* Pet. 63–77. In support, Petitioner relies on the testimony of Dr. Houh and provides citations to the reference teachings. *Id.*

On this record, Petitioner persuasively maps the steps of claims 22–24, 28, and 29 to the asserted prior art and provides reasons supported by factual underpinnings of record to combine the reference teachings with a reasonable expectation of success. *See id.*

Patent Owner does not address these claims separately, but groups claims 19 and 23 together, relying on the same unavailing arguments regarding the "VPN tunnel" limitations addressed above in connection with claim 19. *See* PO Resp. 20–27.

Accordingly, we determine that Petitioner shows by a preponderance of evidence that claims 22–24, 28, and 29 would have been obvious based on the combined teachings of Knappe, Elliott, VPN Textbook, Hendricks, and Drell.

## IV. CONCLUSION

For the reasons discussed above, Petitioner has shown by a preponderance of the evidence that claims 19–29 of the '612 patent are unpatentable.[11] The following table summarizes our conclusions:

| Claim(s) | 35 U.S.C. § | Reference(s)/ Basis | Claim(s) Shown Unpatentable | Claim(s) Not shown Unpatentable |
|---|---|---|---|---|
| 19–21, 25–27 | 103(a) | Knappe, Elliott, VPN Textbook, Hendricks | 19–21, 25–27 | |
| 22–24, 28, 29 | 103(a) | Knappe, Elliott, VPN Textbook, Hendricks, | 22–24, 28, 29 | |

[11] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3), (b)(2).

| | | | | |
|---|---|---|---|---|
| | | Drell | | |
| **Overall Outcome** | | | 19–29 | |

## V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that Petitioner establishes by a preponderance of evidence that challenged claims 19–29 are unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Hector J. Ribera
C.J. Alice Chuang
MARTON RIBERA SCHUMANN & CHANG LLP
hector@martonribera.com
cjalice@martonribera.com

PATENT OWNER:

Gregory S. Donahue
Andrew G. DiNovo
DINOVO PRICE LLP
gdonahue@dinovoprice.com
adinovo@dinovoprice.com