UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

POLYCOM, INC.,
Petitioner,

v.

DIRECTPACKET RESEARCH, INC.,
Patent Owner.

IPR2019-01235
Patent 8,560,828 B2

Before BRYAN F. MOORE, SHEILA F. McSHANE, and RUSSELL E. CASS, *Administrative Patent Judges*.

CASS, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

Polycom, Inc. ("Petitioner") filed a Petition pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–23 of U.S. Patent No. 8,560,828 B2 ("the '828 patent"). Paper 1 ("Pet."). directPacket Research, Inc. ("Patent Owner") filed a Preliminary Response to the Petition. Paper 7. Pursuant to 35 U.S.C. § 314, we instituted *inter partes* review of all of the challenged claims based on all the grounds presented in the Petition. Paper 19 ("Inst. Dec.").

Patent Owner filed a Response (Paper 28, "PO Resp."), Petitioner filed a Reply (Paper 44, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 57, "PO Sur-reply"). On October 20, 2020, we conducted an oral hearing. A copy of the transcript of the oral hearing (Paper 68, "Tr.") is included in the record. Following the oral hearing, we issued an Order allowing additional briefing on the proper construction of the term "multimedia communication data" in certain claims. Paper 68. Pursuant to the Order, Petitioner and Patent Owner filed supplemental briefs directed to claim construction (Paper 64, "PO Supp."; Paper 65, "Pet. Supp.") and responses (Paper 66, "Pet. Supp. Resp."; Paper 67, "PO Supp. Resp.").

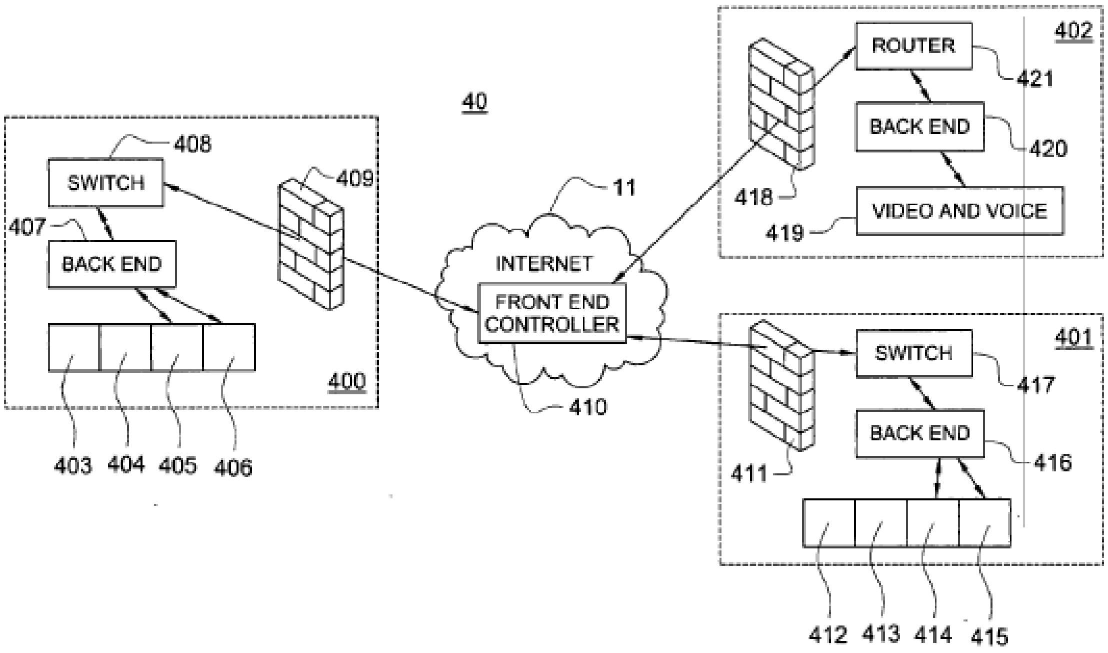
We have jurisdiction under 35 U.S.C. § 6(b). For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–23 of the '828 patent are unpatentable. This final written decision is issued pursuant to 35 U.S.C. § 318(a).

I. BACKGROUND

A. The '828 Patent (Ex. 1001)

The '828 patent is entitled "System and Method for a Communication System" and issued on October 15, 2013, from an application filed on April 13, 2006. Ex. 1001, codes (22), (45), (54). The '828 patent is directed to a system and method for managing a communication system. Ex. 1001, 5:14–15. The communication system may include one or more communication communities having endpoints connected into the community. *Id.* at 5:15–18. Figure 4, reproduced below, is a block diagram of a communication community.

FIG. 4



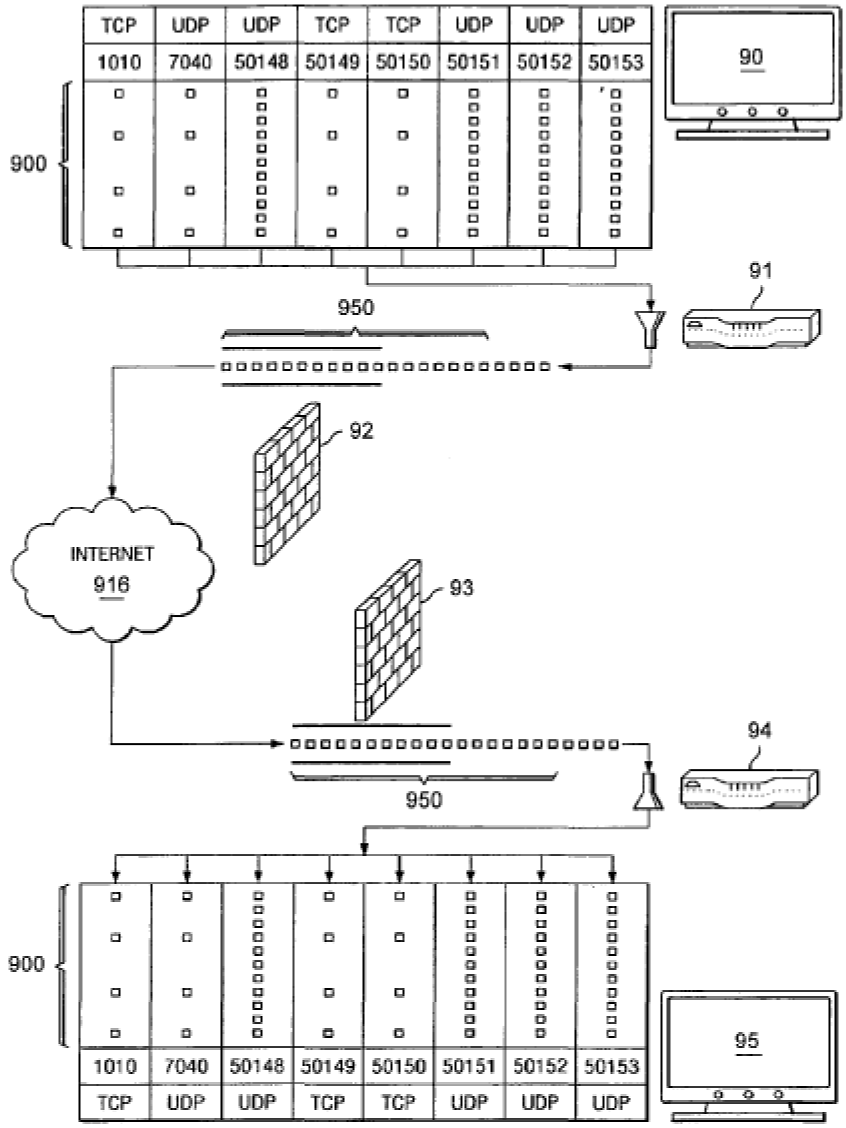
In Figure 4, principal office 400 is a company's principal business location, satellite office 401 is a branch office located in a suburb of the city where principal office 400 is located, and travel office 402 is a hotel room in another location across the country where the company's CEO is attending a company meeting. *Id.* at 6:53-63. Each location has a firewall (409, 411, and 418, respectively) connected to one or more endpoints (403–406, 419, and 412–415, respectively) through switches, routers, and a back end controller. *Id.*at 7:1–8, 7:20–22. Back end controller 407 manages the communication interactions with endpoints 403–406 and allows communication from the endpoints to be transmitted to switch 408 and firewall 409, and eventually out to Internet 11 and front end controller 410. *Id.* at 7:5–8. Front end controller 410 is located outside of firewall 409. *Id.* at 10:15.

The ’828 patent discloses another embodiment which creates a scaled communication network by combining or joining the communication capabilities of several communication sub-systems (each including a front-end controller) into a single “expanded community.” *Id.* 11:1–61, Fig. 5. Yet another embodiment uses one of the front-end controllers in one of the sub-systems as a “super controller” that acts as the main front end controller and operates as a conduit for the other sub-systems. *Id.* 12:31–47.

The ’828 patent explains that in order to implement Voice over Internet Protocol (VoIP), new transmission protocols have been developed for multimedia communication, including Session Initiation Protocol (SIP) and H.323. *Id.* at 2:57–62. However, the patent explains, these protocols run into problems when encountering firewalls because the protocols use multiple different ports that can be dynamically selected as the session is initiated, but the majority of these ports are closed in typical firewall installations. *Id.* at 2:67–3:8. Opening too many ports, the patent explains, would risk exposure of an entity to potentially harmful unauthorized intrusion. *Id.* at 3:10–12.

The ’828 patent seeks to overcome this potential problem by using a system that converts the multiport packets sent on multiple ports (multiport packets) to packets sent on a single port (single-port packets) for transmission through a firewall. *Id.* at 7:33–37. Such a system is illustrated in Figure 9, reproduced below.

FIG. 9



In Figure 9, video conference endpoint 90 attempts to send multimedia packets 900 to video conference endpoint 95, using back end controllers 91 and 94. *Id.* at 8:4–10. Controller 91 receives multiport packets 900 from endpoint 90, encapsulates each of them into single-port packets 950, and sends single-port packets 950 to back end controller 94. *Id.* at 8:26–8:30. Firewall 92 inspects the traffic from device 91 before sending it out through Internet 916 to controller 94. *Id.* at 8:44–45. Controller 94 receives the encapsulated single-port packets 950 and then reconstructs multiport packets 900 from the single-port packets 950. *Id.* at 8:49–51.

B. Illustrative Claims

Three of the challenged claims of the '828 patent, claims 1, 11, and 17, are independent. Claim 1, which is illustrative, is reproduced below, with reference letters in brackets added at the beginning of each sub-paragraph to allow ease of reference throughout this Decision.

> 1. A method for a multimedia communication comprising:
>
> [a] receiving, at a controller that is behind a firewall and that is communicatively coupled with a plurality of endpoint communication devices, a plurality of multiport packets of data in a multiport communication protocol for communication from at least one of the plurality of endpoint communication devices;
>
> [b] converting, by said controller, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol;
>
> [c] receiving at an external controller a communication request from said controller behind said firewall, wherein said external controller is not behind said firewall;
>
> [d] establishing a communication channel between said controller and said external controller;
>
> [e] opening a second communication channel between said external controller and at least one other controller behind another firewall, wherein said at least one other controller is configured to service a single endpoint communication device;
>
> [f] transmitting multimedia communication data between said controller and said at least one other controller wherein said multimedia communication data passes through said external controller; and
>
> [g] distributing said multimedia communication data to one or more of said plurality of endpoint communication devices and said single endpoint communication device.

Ex. 1001, 13:64–14:25.

C. The Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–23 of the ’828 patent on the following grounds:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1, 3–5, 9–11, 13, 14, 16, 17, 22, 23	103(a)[1]	Krtolica,[2] Rosenberg[3]
2, 12, 18, 19	103(a)	Krtolica, Rosenberg, Eisenberg[4]
6–8, 15, 20	103(a)	Krtolica, Rosenberg, DSDP[5]
21	103(a)	Krtolica, Rosenberg, Eisenberg, DSDP

Pet. 6.

Petitioner also submits a declaration of Tal Lavian with its Petition (Ex. 1002) and a supplemental declaration of Tal Lavian in support of its Reply (Ex. 1042). Patent Owner submits a declaration of Kevin Jeffay (Ex. 2009) and a declaration of Rahul Vijh (Ex. 2008) in support of its Response.

D. Related Proceedings

At the time of the filing of the Petition, Petitioner identified *directPacket Research, Inc. v. Polycom, Inc.*, 2:18-cv-00331-AWA-RJK (E.D. Va.), as a related matter. Pet. 3. At the time of the filing of

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the challenged claims of the ’828 patent have an effective filing date before the effective date of the applicable AIA amendment, we refer to the pre-AIA version of 35 U.S.C. § 103.

[2] US 7,360,243 B2, issued April 15, 2008 (Ex. 1004).

[3] J. Rosenberg, *SIP Traversal Through Residential and Enterprise NATs and Firewalls*, Internet Engineering Task Force, November 17, 2000 (Ex. 1005).

[4] U.S. 7,979,528 B2, issued July 12, 2011 (Ex. 1006).

[5] *Designing a Static Dial Plan*, Cisco Technology White Paper, Version 2, October 25, 2001 (Ex. 1007).

Mandatory Notices, Patent Owner indicated that *directPacket Research, Inc. v. Polycom, Inc.*, C.A. No. 5:19-cv-03918-VKD (N.D. Cal.), involved the ’828 patent. Paper 4, 2 (Notices). As discussed in the Institution Decision, the parties both refer to a single litigation (“the district court litigation”), which was originally filed in the Eastern District of Virginia and was then transferred to the Northern District of California in July 2019. Inst. Dec. 3, 12–13.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

The Petition asserts that a person of ordinary skill in the art (POSA) would have had a “a Bachelor’s degree or equivalent in electrical engineering, computer engineering, or similar field, and at least two years’ experience in a relevant field such as telecommunications or multimedia communications.” Pet. 27–28. In support, Dr. Lavian testifies that the relevant experience could include “experience in designing, implementing, monitoring and maintaining [voice over Internet protocol (VoIP)] and multimedia networks,” and the person of ordinary skill would therefore have “at least some familiarity with the fundamentals of computer networks and related concepts, including VoIP, multimedia transmissions, protocol conversion, and well-known communication protocols such as SIP, H.323, and TCP/IP.” Ex. 1002 ¶ 18.

In our Institution Decision, we adopted Petitioner’s proposed skill level, that is, that one of ordinary skill in the art should have a Bachelor’s degree or equivalent in electrical engineering, computer engineering, or similar field, and at least two years of experience in a relevant field such as telecommunications or multimedia communications. Inst. Dec. 21. We also agreed that one of ordinary skill would have some familiarity with the design and implementation of VoIP and multimedia networks, finding that these qualification are commensurate with the relevant technology and claims of the ’828 patent, as well as that of the asserted prior art. *Id.* at 21–22. However, we agreed with Patent Owner’s argument in the Preliminary Response that the qualifications did not include monitoring and maintaining VoIP and multimedia networks, as Petitioner asserts, and therefore declined to adopt that requirement as part of the definition of a person of ordinary skill. *Id.* at 22.

In its Patent Owner Response, Patent Owner states that it “accepts the Board’s characterization of one of ordinary skill in the art in so far as the proscribed ‘familiarity with the design and implementation of VoIP and multimedia networks’ would have provided the skilled artisan with” an understanding of certain matters. PO Resp. 23. These matters include: “the issues faced when performing multimedia communications over existing data networks”; “the techniques employed by network firewalls and network address translation (‘NAT’) devices, and the issues they present with respect to establishing and conducting multimedia communication sessions”; “the performance demands placed on the network by multimedia communications, and the constraints that such demands place on the processing that can be performed”; and “the distinctions between existing firewall traversal solutions, such as ALG, VPN tunnels, and the inventions of the ’828 Patent.” *Id.* Petitioner does not further discuss or comment on Patent Owner’s statement regarding the person of ordinary skill.

Based on the full record developed during trial, including our review of the ’828 patent and the types of problems and solutions described in the ’828 patent, the prior art, and the testimony of the parties’ declarants, we maintain our finding on the level of ordinary skill in the Institution Decision. Accordingly, we find that one of ordinary skill in the art would have a Bachelor's degree or equivalent in electrical engineering, computer engineering, or similar field, and at least two years of experience in a relevant field such as telecommunications or multimedia communications, and would have some familiarity with the design and implementation of VoIP and multimedia networks. We would reach the same result on the ultimate question of obviousness of the '828 patent whether or not we adopt Patent Owner's statements in its Response of the matters that would be understood by a person of ordinary skill based on their familiarity with the design and implementation of VoIP and multimedia networks.

B. Claim Construction

In an *inter partes* review for a petition filed on or after November 13, 2018, as here,

> claim[s] of a patent . . . shall be construed using the same claim construction standard that would be used to construe the claim[s] in a civil action under 35 U.S.C. § 282(b), including construing the claim[s] in accordance with the ordinary and customary meaning of such claim[s] as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

See Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340, 51358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005).

The parties dispute the meaning of the term "multimedia communication data" in challenged claims 1, 5, 6, 7, and 8. Patent Owner argues that "multimedia communication data" "must be construed to include both signaling and media messages." PO Supp. 1. Petitioner, on the other hand, argues that "multimedia communication data" does not have to include both signaling and media messages and may include signaling alone. Pet. Supp. 1.

More specifically, Petitioner argues that the "plain and ordinary meaning of multimedia communication data is simply data related to multimedia communications," and this data "may be signaling or it may be media content or both." Pet. Supp. 1. Petitioner states that the Specification does not expressly define "multimedia communications data," but argues that the Specification supports Petitioner's understanding of the term's ordinary meaning because it describes embodiments that only carry signaling, specifically embodiments using SIP and H.323 protocols. *Id.* at 2–3. Thus, according to Petitioner, interpreting "multimedia communication data" to exclude messages that contain only signaling for the multimedia transmission would read out the '828 patent's SIP and H.323 embodiments. *Id.* Petitioner further argues that the '828 patent incorporates by reference Patent Owner's U.S. Patent No. 7,710,978 B2, which also discloses controllers that may communicate using signaling only, including H.323 gatekeepers and gateways, and SIP proxies and registrars. *Id.* at 3. Petitioner additionally relies on testimony from Dr. Lavian that SIP and H.323 operate with signaling channels that do not carry media content. *Id.* at 3–5.

Turning to Patent Owner's position, Patent Owner argues that "the plain language of the claim dictates that 'multimedia communication data' be construed to include media," and "constru[ing] 'multimedia' to mean *no* media improperly rewrites the plain language of the claim to exclude the word 'multimedia.'" PO Supp. 2. Thus, according to Patent Owner, "'multimedia communication data' must include media messages to give effect to the word 'multimedia.'" *Id.* Patent Owner argues that its construction is supported by the Specification's reference to "media traffic" as including "voice, video, and the like" and "data for the images and sound being transmitted between endpoints." *Id.* at 3 (citing Ex. 1001, 7:48–55). Patent Owner further argues that Figures 4, 5, and 8 of the '828 patent illustrate the "multimedia communication data" passing through the external controller on a single path, not two separate paths for signaling and media messages. *Id.* (citing Ex. 1001, Figs. 4, 5, 8). As for Petitioner's argument that Patent Owner's construction would read out the '828 patent's SIP and H.323 embodiments, Patent Owner argues that this argument "rests on a faulty premise" because "H.323 is a suite of protocols including both signaling and media protocols" and, similarly, "SIP is understood as a family of protocols that convey both signaling and media messages." *Id.* at 4–5.

We find that the evidence supports Petitioner's construction. Starting with the claim language itself, we agree with Petitioner that the ordinary meaning of "multimedia communication data" is data related to multimedia communication, and that this may comprise signaling data required for communicating multimedia between two or more locations. We see nothing in the claim language that requires that data must include the underlying media content itself (such as video or voice signals) in order to qualify as "multimedia communication data." We also are not persuaded by Patent Owner's argument that Petitioner's construction of "multimedia" "means no media" (PO Supp. 1 (emphasis omitted)), because Petitioner is not arguing that media content cannot be present, but instead is simply arguing that media content is one type of "multimedia communication data," with another type being signaling data used for multimedia communication. *See* Pet. Supp. Rep. 1.

Petitioner's construction is also supported by the written description. Although the Specification does not contain an express definition of "multimedia communication data," it includes examples of using signaling protocols, such as SIP and H.323, for multimedia communication. *See* Ex. 1001, 2:59–62, 3:4–24, 7:27–37. For example, the Specification explains as follows:

> In order to implement VoIP [(Voice over IP)], . . . new transmission protocols were developed to handle the specific needs of such system[s]. ***Session Initiation Protocol (SIP) and H.323 are two examples of such protocols that have been defined for*** handling the administration of VoIP, and its natural extension to ***multimedia communication***.

Ex. 1001, 2:57–62 (emphasis added).

The Specification goes on to state that "SIP is a ***signaling protocol*** for Internet conferencing, telephony, presence, events notification, and instant messaging," and "H.323 is a multimedia conferencing protocol, which includes voice, video, and data conferencing, for use over packet-switched networks." *Id.* at 2:63–67 (emphasis added); *see also id.* at 3:4–24 (describing the use of H.323 and SIP), 3:33–34 (referring to SIP and H.323 as "multimedia transport protocol[s]"). The Specification further explains that SIP and H.323 send signaling messages for the multimedia data separate from the media itself. *See* Ex. 1001, 7:38–51 (explaining that H.323 and SIP "specify different types of traffic that may be sent between endpoints which include media traffic (voice, video, and the like) along with the control traffic (camera, connection control, and the like)").

In addition, the Specification discloses that SIP and H.323 may be used in embodiments of the present invention. *Id.* at 7:27–35 ("back end controller 407" in Figure 9 may use "multiport transport protocols, such as H.323, SIP, and the like"), 9:32–35 (endpoint 90 in the system registers with backend controller 91 by "identifying itself as a compliant endpoint (e.g., it is an endpoint that conforms to H.323, SIP, VoIP, or the like")); *see also* Ex. 2050, U.S. Patent No. 7,710,978 B2 (incorporated by reference in Ex. 1001, 1:7–12) at 6:40–44 (stating that its firewall traversal system can be connected to "H.323 gatekeepers, H.323 gateways, SIP proxies, SIP registrars, or the like"), 6:55–59 (network device 21 may be integrated into other network devices, including "H.323 gateways, SIP proxies, SIP registrars or the like"). "[T]here is a strong presumption against a claim construction that excludes a disclosed embodiment." *See In re Katz Interactive Call Processing Patent Litig.*, 639 F.3d 1303, 1324 (Fed. Cir. 2011). Thus, because the Specification discloses, in certain embodiments, the use of signaling protocols only (such as SIP) in its multimedia communications, it supports a claim construction for the term "multimedia communication data" that includes signaling messages only.

We also credit Dr. Lavian's testimony, which is in accord with the Specification. Dr. Lavian testifies that "H.323 and SIP are signaling protocols that operate by setting up a signaling path to initiate and control connections." Ex. 1042 ¶ 5. Dr. Lavian further explains that SIP does not transmit multimedia content, and "[i]n SIP and H.323, RTP [(Real-time Transport Protocol)] is used to transmit the multimedia data while SIP and H.323 provide signaling and control." Ex. 1042 ¶ 7. Thus, according to Dr. Lavian, "SIP, for example, does not transmit the actual media, so when the '828 patent discusses a 'SIP packet data' (Ex. 1001, 3:19)[,] it is necessarily referring to a packet of SIP messaging that sets up and controls the RTP channel, not the actual communication data." *Id.* Dr. Lavian explains that "[t]his is defined in the IETF standard 'SIP-H.323 Internetworking' from July 2001." *Id.* ¶ 8 (citing IPR2019-01233, Ex. 1010).

We also rely on Dr. Jeffay's testimony, which is in agreement with that of Dr. Lavian. Dr. Jeffay testifies that

> ***SIP*** is only used to establish sessions. It ***does not carry the actual media*** for the session. As such, ***SIP is considered a "signaling" protocol*** as it generates the "signals" (messages) to set up and manage a call. . . . ***RTP, or Real-Time Transport Protocol***, is an application layer protocol ***for actually carrying the media*** of a multimedia communication session.

Ex. 2009 ¶¶ 75–76 (emphasis added). We credit Dr. Lavian's and Dr. Jeffay's testimony on this point because they are in substantial agreement and the testimony is consistent with the disclosures of the Specification.

Patent Owner responds by arguing that "[t]he '828 Patent expressly refers to each of SIP and H.323 as a family of protocols which transmit *both* signaling and media to enable multimedia communication," and that "[t]here is no record evidence that would support a finding by the Board that any embodiment of the '828 patent requires the transmission of signaling messages alone to enable the claimed methods of multimedia communication." PO Supp. Resp. 2. We do not find this argument persuasive. Petitioner does not argue that the '828 patent *requires* the transmission of signaling messages alone to enable the claimed methods of multimedia communication, but rather argues that the '828 patent discloses embodiments that include separate signaling and media messages. Patent Owner does not point to evidence refuting Petitioner's showing that the '828 patent's disclosure of SIP and H.323 encompasses embodiments where signaling messages are transmitted separately from media messages. Indeed, Patent Owner's own expert, Dr. Jeffay, agrees that SIP is a "signaling" protocol that "does not carry the actual media for the session." Ex. 2009 ¶¶ 75–76.

We are also not persuaded by Patent Owner's argument that the Specification describes "media traffic" as being "voice, video and the like." PO Supp. 3 (quoting Ex. 1001, 7:48–55). The claims do not use the term "media traffic," but rather use the term "multimedia communication data," and the Specification does not equate the terms or indicate that "multimedia communication data" should be limited to only "media traffic." Similarly, we are not persuaded by Patent Owner's argument that Figures 4, 5, and 8 of the '828 patent show only a single line passing through the external controller, because the use of a single line does not define the types of data that may be transmitted between the controller and external controller, and thus does not preclude the transmission of signaling data, media data, or both.

Finally, Patent Owner argues in a footnote that a person of ordinary skill "would not have understood the claims as covering the transmission of signaling *alone* because signaling is typically only communicated over a single port, whereas the claims require the transmission of '*multiport* packets of data in a *multiport* communication protocol.'" PO Supp. Resp. 2 n.1 (quoting Ex. 2027, 41, 44). However, as discussed above, SIP is a signaling protocol, and the '828 patent describes SIP as a "multiport communication protocol." *See* Ex. 1001, 3:4–6 ("Many communication protocols, including H.323 and SIP, use multiple different ports that can be selected dynamically as the session is initiated."); 7:33–34 (referring to "multiport transport protocols, such as H.323, SIP, and the like"), 7:44–45 (referring to "H.323, SIP, or other similar multimedia communication protocols"). In light of these statements in the Specification, Patent Owner fails to sufficiently explain or present evidence as to why SIP is not a "multiport communication protocol."

Consequently, we construe the term "multimedia communication data" to mean data relating to multimedia communication, which can be signaling alone as well as signaling and media content.

Neither Petitioner nor Patent Owner proposes constructions for any of the remaining claim terms, and we do not find it necessary to expressly construe any other terms for purposes of this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy' . . . ." (citations omitted)).[6]

C. Principles of Law

A claim is unpatentable for obviousness if, to one of ordinary skill in the pertinent art, "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." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a)). The question of obviousness is resolved on the basis of underlying factual determinations, including "the scope and content of the prior art"; "differences between the prior art and the claims at issue"; "the level of

[6] To the extent the parties' disputes concerning whether certain limitations are satisfied by the prior art arguably implicate claim construction issues, those disputes are addressed further below in the sections discussing application of the prior art to the claim limitations.

ordinary skill in the pertinent art"; and objective indicia of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

A patent claim "is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. An obviousness determination requires finding "both 'that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.'" *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016) (citation omitted); *see KSR*, 550 U.S. at 418 (For an obviousness analysis, "it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does."). Further, an assertion of obviousness "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (A finding of a motivation to combine "must be supported by a 'reasoned explanation.'" (citation omitted)).

D. Ground 1: Obviousness over Krtolica and Rosenberg — Claims 1, 3–5, 9–11, 13, 14, 16, 17, 22, and 23

Petitioner contends that claims 1, 3–5, 9–11, 13, 14, 16, 17, 22, and 23 are unpatentable as obvious under 35 U.S.C. § 103(a) over Krtolica and Rosenberg. Pet. 30–70. For the reasons that follow, Petitioner has demonstrated by a preponderance of the evidence that claims 1, 3–5, 9–11, 13, 14, 16, 17, 22, and 23 are unpatentable on this ground.

1. Overview of Krtolica

Krtolica is directed to a system that sends information data packets from multiple send endpoint ports to multiple receive endpoint ports by converting the packets into a single stream and sending them through a selected port in at least one firewall. Ex. 1004, 3:55–62. Figure 1, reproduced below, depicts an embodiment of Krtolica's system:

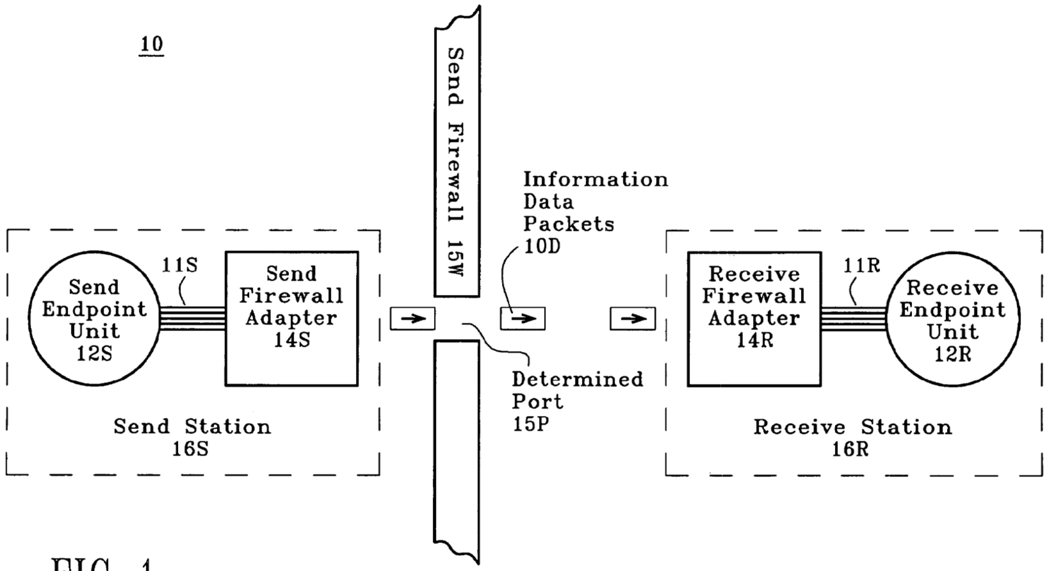

10
Send Firewall 15W
Information Data Packets 10D
Send Endpoint Unit 12S
11S
Send Firewall Adapter 14S
Send Station 16S
Determined Port 15P
Receive Firewall Adapter 14R
11R
Receive Endpoint Unit 12R
Receive Station 16R

FIG 1

Figure 1, above, depicts standard based communication system 10 supporting firewall-friendly communication between send station 16S and receive station 16R. Ex. 1004, 3:64–67. Endpoint ports 11S are shown in send endpoint unit 12S with packets passing through standard based send firewall adapter 14S, traversing firewall 15W through selected port 15P, and passing through standard based receive firewall adapter 14R. *Id.* at 3:55–62. The endpoint units in the send and receive stations may be simple PCs operated by individuals at a single work station, a collection of end user PCs and other standard based communication devices, or complex computer system(s) operated by large organizations. *Id.* at 4:1–6.

Figure 3, reproduced below, is a block diagram of the firewall adapters in Figure 1. Ex. 1004, 2:62–63.

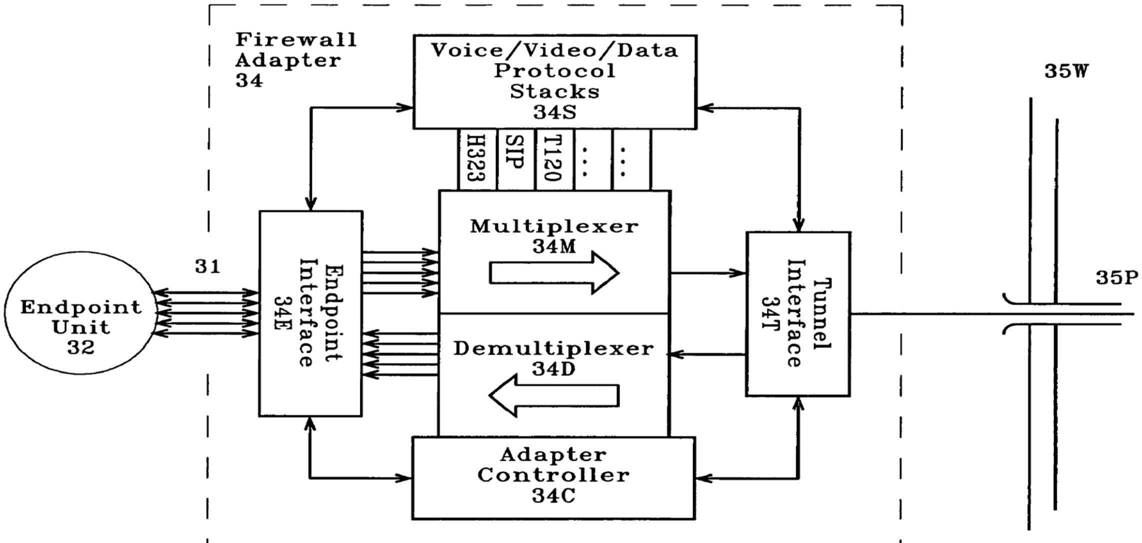


FIG 3

As shown in Figure 3, above, firewall adapter 34 includes endpoint interface 34E and tunnel interface 34T, which manages the transport of incoming and outgoing data packets. Ex. 1004, 4:41–45. Multiplexer 34M reads the header configuration of outgoing packets in multiple streams of packets from multiple send endpoint ports 31 of send endpoint unit 32, and provides a single stream of multiplexed packets, which traverse firewall 35W through port 35P. *Id.* at 4:57–61. Demultiplexer 34D reads the header configuration of incoming packets in the single stream of received packets that has traversed the firewall and provides multiple streams of demultiplexed packets for multiple endpoint ports 31. *Id.* at 4:62–66.

Figure 4, reproduced below, is a block diagram showing a send firewall adapter (like Adapter 14S in Fig. 1) sending data packets through a network port to a receive firewall adapter (like Adapter 14R in Fig. 1):

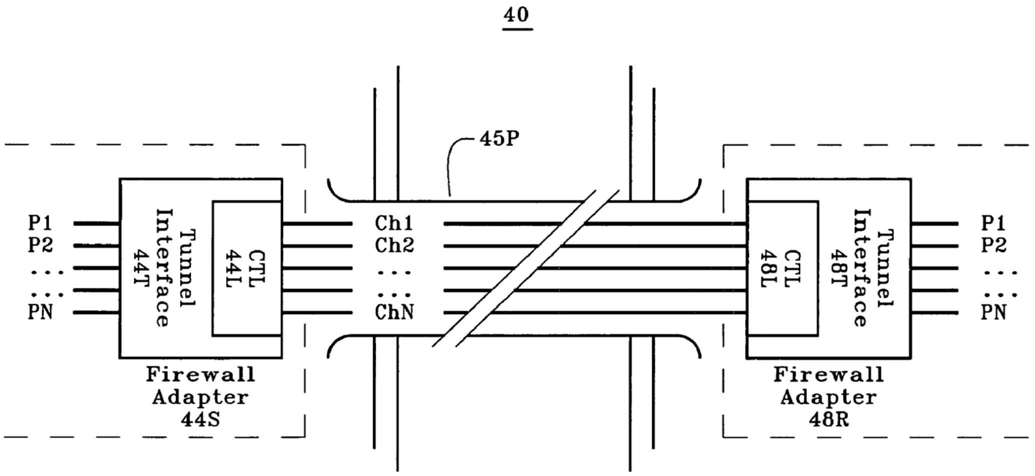


FIG 4

Figure 4, above, depicts system 40 that distributes information data packets from multiple send endpoint ports P1, P2, . . . Pn within send firewall adapter 44S, to multiple receive endpoint ports P1, P2, . . . Pn within receive firewall adapter 48R. Ex. 1004, 5:9–12. The data packets enter tunnel interface 44T on the multiple send ports, and leave on multiple corresponding logical channels C1, C2, . . . Cn. *Id.* at 5:12–15. The port to channel conversion is effected by component and template library (CTL) 44L within the tunnel interface that assigns a unique channel number to the headers of the outgoing data packets arriving from each send port. *Id.* at 5:15–19. All of the assigned channels are tunneled to receive firewall adapter 48R in common network port 45P, which is typically port 80. *Id.* at 5:19–21.

Figure 2, reproduced below, shows a system for communicating between various locations across a communication network such as the Internet. *Id.* at 3:64–67.

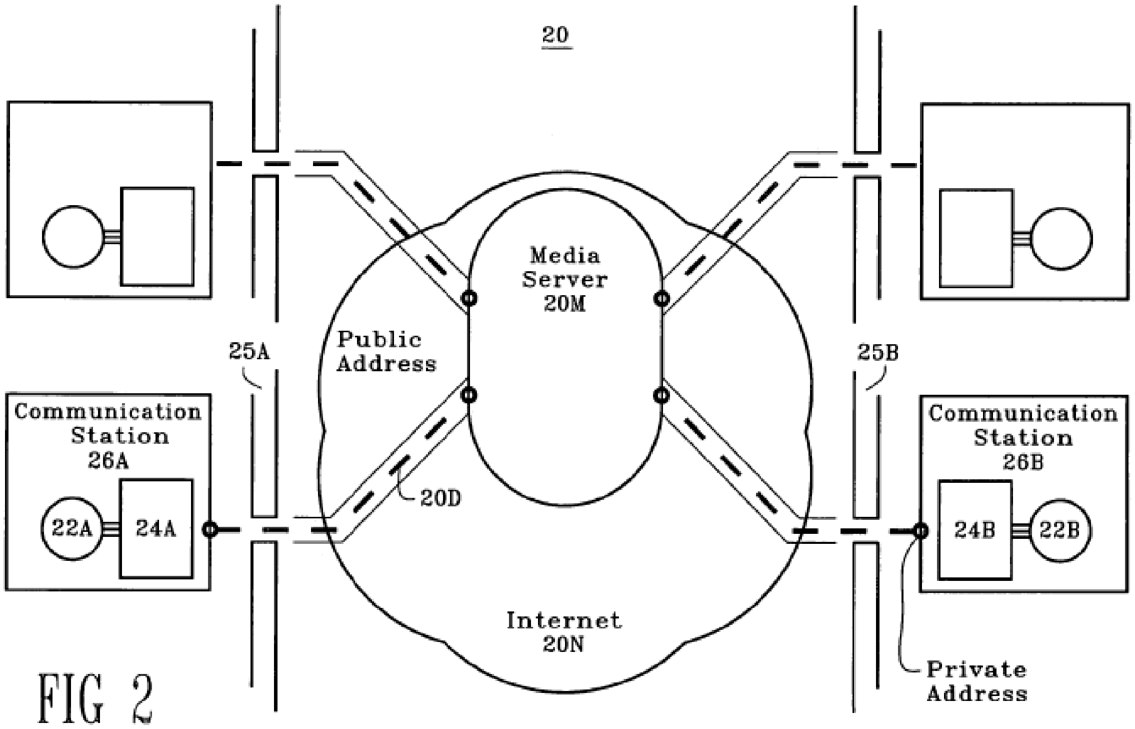


FIG 2

In Figure 2, above, system 20 distributes information data packets 20D from endpoint unit 22A to endpoint unit 22B. *Id.* at 4:11–12. The packets pass through firewall adapter 24A, traverse firewall 25A, and enter Internet 20N. *Id.* at 12–14. The packets are processed by media server 20M, traverse firewall 25B, and pass through firewall adapter 24B. *Id.* at 4:14–16. Krtolica discloses that Internet 20N may contain media servers for providing communication functions such as NAT (network address translations), and that the media server may be accessed by hundreds of parties simultaneously, each of which may have a firewall with a firewall adapter. *Id.* at 4:26–28, 32–34.

2. *Overview of Rosenberg*[7]

Rosenberg is an Internet-Draft from the Internet Engineering Task Force (IETF) titled "SIP Traversal through Residential and Enterprise NATs and Firewalls." Ex. 1005, 1. Rosenberg describes a network architecture in Figure 1, which is reproduced below:

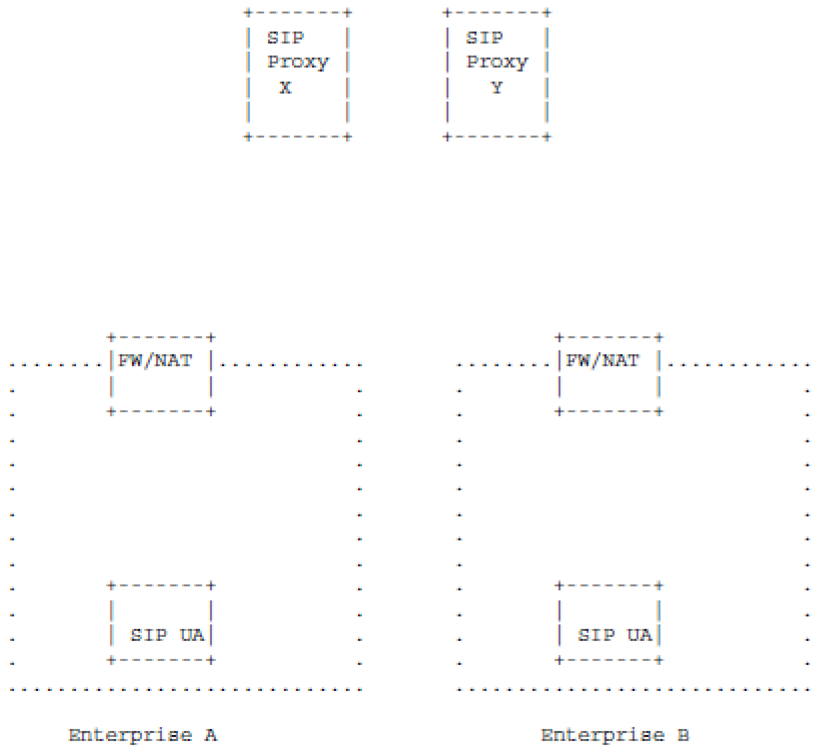


Figure 1: Network Architecture

Ex. 1005, 3.

[7] In the Preliminary Response, Patent Owner disputed the authenticity and printed publication status of Rosenberg. Prelim. Resp. 27–35, 39–50. No arguments on this issue were presented in the Patent Owner Response. *See generally* PO Resp. We ordered that "any arguments for patentability not raised in the [Patent Owner] response may be deemed waived," and we deem any arguments not raised in the Response to be waived by Patent Owner. Paper 20, 8. *See Novartis AG v. Torrent Pharms. Ltd.*, 853 F.3d 1316, 1330 (Fed. Cir. 2017); *In re NuVasive*, 842 F.3d at 1381.

In Figure 1, the caller is represented by SIP UA (user agent) in Enterprise A, and the called party is represented by SIP UA in enterprise B. *Id.* at 2. The boxes labeled "FW/NAT" represent firewalls. *Id.* at 2–3. The caller uses SIP Proxy X, which is outside the firewall, as its local outbound proxy, which forwards the call to the proxy of the called party, Y, also outside a firewall. *Id.* at 2. The call is then forwarded to the called party within Enterprise B. *Id.*

Rosenberg also discloses various network security features. For example, Rosenberg discloses that all HTTP (Hypertext Transfer Protocol) messages are encrypted, and that the firewall never sees any HTTP messages in the clear, only TLS/SSL messages. *Id.* at 4. Rosenberg further discusses the use of a TLS (transport layer security) server process using a public-private/key:

> Our approach requires a TLS server process (to receive RTP) embedded within a SIP enabled communications client. This will require a public/private key and its associated certificate, available to the client, issued from a Certification Authority (CA) that is known to the other party. Similarly, use of a TLS client will require that the client be configured with the keys of a set of well[-]known CAs.

Id. at 12.

3. *Claim 1*

a. *"A method for a multimedia communication comprising:"*

Petitioner asserts that Krtolica teaches a method for multimedia communication, as recited in the preamble of claim 1. Pet. 31. Petitioner relies upon Krtolica's disclosure of multimedia communications between Send Endpoint Unit 12S and Receive Endpoint Unit 12R, as well as

Krtolica's statement that the invention "relates to routing voice/video/data communications through network firewalls." *Id.* (quoting Ex. 1004, 1:7–8).

Patent Owner does not address Petitioner's showing as to the preamble; therefore, any such arguments are waived. *See Novartis AG v. Torrent Pharms. Ltd.*, 853 F.3d 1316, 1330 (Fed. Cir. 2017); *In re NuVasive*, 842 F.3d at 1381.[8] Based on the entirety of the record, we find that Petitioner has shown that Krtolica teaches the language in the preamble of claim 1.[9]

b. Limitation 1[a]: "receiving, at a controller that is behind a firewall and that is communicatively coupled with a plurality of endpoint communication devices, a plurality of multiport packets of data in a multiport communication protocol for communication from at least one of the plurality of endpoint communication devices"

Petitioner asserts that Krtolica teaches the claimed "controller" in the form of send firewall adapters, such as send firewall adapter 14S of Krtolica's Figure 1. Pet. 31–32 (citing Ex. 1004, Fig. 3 at firewall adapter 34, 3:55–67, Fig. 2 at 24A, Fig. 4 at 44S). Petitioner asserts that Krtolica teaches that its firewall adapters may be communicatively coupled with a plurality of endpoint communication devices in the form of endpoint units, such as endpoint unit 12S in Figure 1 and 32 in Figure 3. *Id.* at 33 (citing Ex. 1004, Figs. 1 and 3). Petitioner further contends that although Figure 1

[8] As in *NuVasive*, the Scheduling Order in this proceeding cautioned Patent Owner that "any arguments for patentability not raised in the response may be deemed waived." Paper 20, 8.

[9] Because Petitioner has sufficiently demonstrated that Krtolica discloses the preamble, we need not and do not decide whether the preamble is limiting for purposes of this Decision.

shows firewall adapter 14S to be communicatively coupled to a single send endpoint unit 12S, Krtolica is clear that the endpoint unit can comprise either one or multiple endpoint devices, such as host computers, a collection of end user PCs, or complex computer systems operated by large organizations. *Id.* (citing Ex. 1004, 1:21–23; 4:1–6).

Petitioner additionally contends that Krtolica discloses a plurality of multiport packets of data in a multiport communication protocol for communication from at least one of the plurality of endpoint communication devices, as shown in Figure 3, where multiple streams of packets are sent from endpoint units 32 using multiple send endpoint ports 31. *Id.* at 34. According to Petitioner, Krtolica also discloses the use of multiport communication protocols including H.323 and SIP, which the '828 patent identifies as multiport communication protocols. *Id.* (citing Ex. 1001, 3:4–6).

Patent Owner does not specifically address Petitioner's showing as to limitation 1[a]. Based on the entirety of the record, we find that Petitioner has shown, by a preponderance of the evidence, that Krtolica teaches this limitation.

c. Limitation 1[b]: "converting, by said controller, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol"

Petitioner contends that limitation [b] of claim 1 is taught by Krtolica's disclosure of "distribut[ing] information data packets from multiple send endpoint ports P1, P2, . . . Pn" by converting them into "multiple corresponding logical channels C1, C2, . . . Cn." *Id.* at 35 (quoting Ex. 1004, 5:9–15, citing 5:19–21). According to Petitioner, the data packets distributed over the "logical channels C1, C2, . . . Cn" of common network port 45P (which is typically port 80) constitute a plurality of single port packets. *Id.* (citing Ex. 1004, 5:9–15 (Data packets from ports P1, P2, . . . Pn "enter tunnel interface 44T on the multiple send ports, and leave on multiple corresponding logical channels C1, C2, . . . Cn."), 5:19–21 ("All of the assigned channels are tunneled to receive firewall adapter 48R in common network port 45P, which is typically port 80.")). Petitioner also contends that Krtolica discloses traversing firewalls using TCP (Transport Control Protocol) and UDP (User Datagram Protocol), which the '828 patent identifies as single-port communication protocols for traversing firewalls. Pet. 36 (citing Ex. 1004, 6:48–7:20; Ex. 1001, 8:21–30).

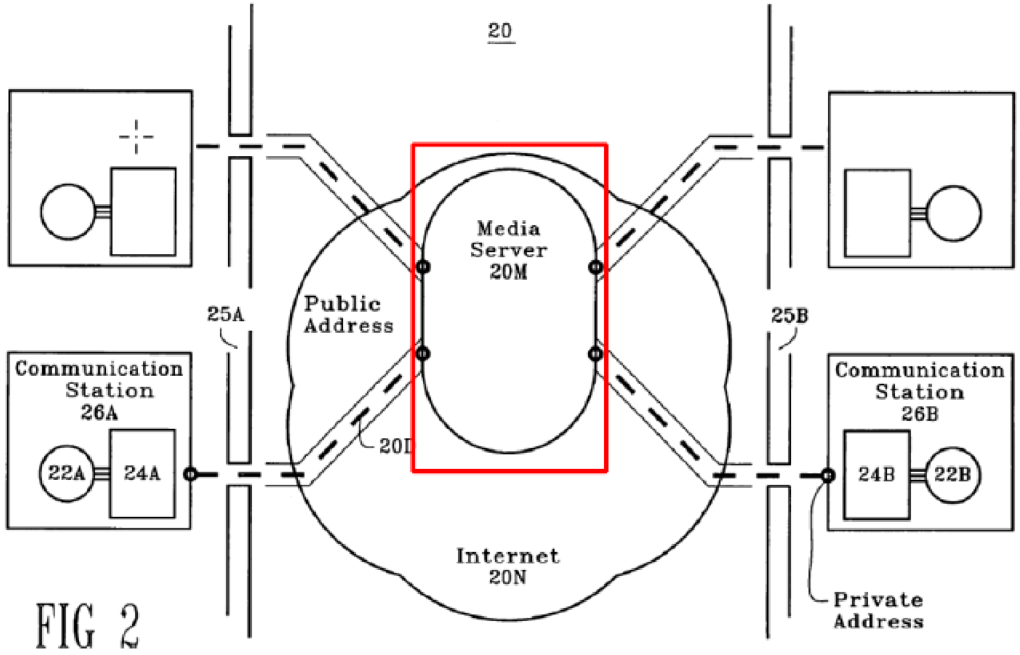
Petitioner further contends that, to the extent one were to determine that Krtolica does not disclose a single-port protocol, Rosenberg discloses the use of a single-port protocol for firewall traversal. *Id.* Relying on the declaration of Dr. Lavian, Petitioner contends that Rosenberg discloses traversing firewalls over default port 443 using HTTPS (Hypertext Transfer Protocol Secure) over TLS/SSL, which is a single-port protocol. *Id.* at 36–37 (citing Ex. 1002 ¶¶ 56–57, 116). Petitioner asserts that the use of HTTPS over port 443 is the same method taught by the '828 patent to traverse firewalls. *Id.* at 37 (citing Ex. 1001, 8:36–39; Ex. 1002 ¶¶ 56, 117).

Petitioner additionally contends that it would have been obvious for a person of ordinary skill to combine Krtolica's teachings regarding firewall traversal with Rosenberg's teachings regarding single-port protocols. *Id.* Relying on the testimony of Dr. Lavian, Petitioner asserts that both references teach similar firewall traversal methods that were well known at the time of the invention, and modifying Krtolica to use HTTPS over port 443 rather than HTTP over port 80 would have been a simple substitution of one known element for another to obtain predictable results. *Id.* (citing Ex. 1004, 6:22–26; Ex. 1002 ¶¶ 57, 117). Furthermore, Petitioner argues, motivation would have existed to use HTTPS (and TLS/SSL) over port 443, as taught by Rosenberg, rather than HTTP (as used in Krtolica) because HTTPS would have provided more secure communication over the Internet than HTTP. *Id.* at 38 (citing Ex. 1004, 1:7–10; Ex. 1001, 2:18–19). Petitioner also relies on the testimony of Dr. Lavian for this point. *Id.* (citing Ex, 1002 ¶¶ 57, 119).

Patent Owner does not address Petitioner's showing as to limitation 1[b]. Based on the entirety of the record, we find that Petitioner has shown, by a preponderance of the evidence, that Krtolica teaches this limitation. We also find that Petitioner has shown that it would have been obvious for a person of ordinary skill to combine Krtolica's teachings regarding firewall traversal with Rosenberg's teachings regarding single-port protocols to meet this claim element.

d. Limitation 1[c]: "receiving at an external controller a communication request from said controller behind said firewall, wherein said external controller is not behind said firewall"

Petitioner contends that limitation [c] of claim 1 is taught by Krtolica. Petitioner contends that Krtolica teaches an "external controller" in the form of media server 20M, which is shown in red in Petitioner's annotated version of Figure 2:



Petitioner's annotated version of Krtolica's Figure 2 showing Media Server 20M in red.

Pet. 39. Petitioner asserts that Media Server 20M is an "external controller" because, as shown in Figure 2, it is on the public Internet and not behind firewall 25A or 25B. *Id.* at 39 (citing Ex. 1004, Fig. 2, 4:10–16, 4:26–28). Petitioner also contends that media server 20M (the "external controller") receives communication requests from firewall adapter 24A, which is behind firewall 25A. *Id.* (citing Ex. 1004, Fig. 2, 4:10–16).

Patent Owner argues that Krtolica fails to disclose "receiving at an external controller a communication request from said controller behind said firewall." PO Resp. 24–25. According to Patent Owner, a person of ordinary skill "would not have understood data packets 10D 'passing' through the firewall adapter and media server, identified as the claimed 'controller' and 'external controller,' respectively, as constituting the exchange of a 'communication request' between the two devices." *Id.* at 25 (citing Ex. 2009 ¶¶ 106–109). This, Patent Owner asserts, is because "both the firewall adapters and media server of *Krtolica* would have been considered passive devices, which may operate on traffic 'passing' through them but do not exchange 'communication requests' between them." *Id.* To the contrary, according to Patent Owner, the '828 patent claims "exchange communication requests from 'a controller behind a firewall' (*i.e.*, a back end controller) to an 'external controller' (*i.e.*, a front end controller)." *Id.* (citing Ex. 2009 ¶ 106). Thus, Patent Owner asserts, Petitioner's position "would lead to a logical absurdity" because it would mean that any pair of in-path communication devices would satisfy this limitation. *Id.* (citing Ex. 2009 ¶ 139).

Petitioner responds that the '828 patent does not set forth a specialized definition of the term "controller," which is simply "a device (or software) on a network that guides or directs the flow of data across the network." Pet. Reply 2–3 (citing Ex. 1001, code (57); Ex. 1042 ¶ 4). Petitioner further argues that the '828 patent discloses embodiments where data "passes through" its controllers, and that Patent Owner's argument would exclude those embodiments from the scope of the claim. *Id.* at 3 (citing Ex. 1001, code (57), Fig. 6 at step 603, 5:36–38). Thus, according to Petitioner, Krtolica discloses limitation 1[c] because its "media server 20M (the external controller) receives data packets 20D (which include communication requests) from firewall adapter 24A (the controller behind a firewall), precisely as claim 1 requires." *Id.* (citing Ex. 1004, Fig. 2, 4:11–16). Petitioner further argues that communication requests "must be received at the media server" because "Krtolica discloses no other path for them to take," and "the media server must establish communication channels with controllers behind firewalls" because "otherwise data packets could not be transmitted between endpoints." *Id.* (citing Ex. 1042 ¶¶ 4–5).

In its Sur-reply, Patent Owner responds that a person of ordinary skill "would have understood the claimed communication request to be used '[i]n establishing the communication configuration in one of the communities/sub-communities,' Ex. 1001, 5:20–23, not for establishing communication between endpoint devices (*i.e.*, communication stations 26A and 26B)." PO Sur-reply 1–2. Patent Owner further argues that Dr. Lavian "admits that the information data packets disclosed in Krtolica may not even contain 'communication requests,' and thus, cannot form the basis for an inherent teaching." *Id.* at 2–3 (citing Ex. 2025, 80:18–21). Patent Owner additionally argues, citing Dr. Jeffay, that "there is no evidence that suggests the Media Server of Krtolica is 'actively involved in [an H.323 or SIP] connection process,'" but rather, "the sole 'communication function[]' disclosed as being performed by Krtolica's Media Server is network address translation (or 'NAT'), . . . which a POSA would have understood to be a 'transparent, connection-less process.'" *Id.* at 3–4 (alterations in original) (citing Ex. 1004, Figs. 2, 4, 4:26–34; Ex. 2009 ¶ 107).

We find that Petitioner has met its burden of showing that claim limitation 1[c] is met by Krtolica. We start with the language of the claim, which states that the external controller "receive[s] . . . a communication request from said controller behind said firewall." We interpret the term "communication request" according to its plain and ordinary meaning to be a request for communication, and find that one of ordinary skill in the art would have understood Krtolica's system as sending a request for communication from the controller behind the firewall (firewall adapter 24A) to Media Server 20M in Figure 2. Krtolica states that data packets are sent from a controller behind a firewall (firewall adapter 24A in Figure 2) to an external controller (media server 20M), where "[t]he packets are processed by media server 20M" before being sent to endpoint unit 22B. Ex. 1004, 4:11–16. Krtolica further states that the media server (external controller) "provid[es] communication functions such as NAT (network address translation)" and that "[t]he send party accesses the visible address at the media server, which routes (translates) the communication to the private address." Ex. 1004, 4:26–32; *see also id.* at 5:23–26 ("During *connection establishment*, CTL 48L [in the firewall adapter] directs tunnel interface 48T to assign the original port number to the headers of the incoming data packets from each channel." (emphasis added)). We find that, based on these disclosures, a person of ordinary skill would have understood that the information received by Krtolica's media server (external controller) includes a request for communication with an endpoint device, and that this is a "communication request" that causes the media server to perform "communication functions such as NAT (network address translation)," which "routes (translates) the communication to" the address of the endpoint receiving the communication.

In reaching this result, we credit the testimony of Petitioner's expert Dr. Lavian. We agree with Dr. Lavian that, "[a]s shown in Krtolica Fig. 2, the media server 20M (the external controller) receives data packets 20D (which include communication requests) from firewall adapter 24A (the controller behind a firewall)." Ex. 1042 ¶ 4. We further rely on and find credible Dr. Lavian's testimony that Krtolica discloses "that the media server processes the packets as they are received at the Media Server and perform services including performing network address translation," because they are consistent with the portions of Krtolica discussed in the previous paragraph. *Id.* ¶ 5 (citing Ex. 1004, 4:14–16, 4:26–28; Ex. 1002 ¶¶ 121–125). Additionally, we rely on Dr. Lavian's testimony that, "[g]iven that

Krtolica discloses H.323 and SIP embodiments, a POSA would understand this processing includes setting up connections" because "H.323 and SIP are signaling protocols that operate by setting up a signaling path to initiate and control connections." *Id.* We find this testimony credible because it is consistent with Krtolica's disclosure of H.323 and SIP as well-known communications standards that are used for voice and video, each of which uses a particular header protocol for communication rules and procedures. As Krtolica explains:

> Currently the three major standard ITU (international telecommunication union) configurations are H323, SIP, and T120. Voice and videos units generally include programs based on H323 or and SIP. Data transfer units (white board applications, file transfers, etc.), are generally T120 based. Each configuration is subject to a particular header protocol of delivery and communication rules and procedures.

Ex. 1004, 1:45–52.

Finally, we find credible Dr. Lavian's testimony that "[c]ommunication requests in Krtolica are necessarily received at the media server" because "Krtolica discloses no other path for them to take" and "the media server must establish communication channels with controllers behind firewalls" because "otherwise data packets could not be transmitted between endpoints." Ex. 1042 ¶ 4. Based on this evidence, we find that a person of ordinary skill would have understood from Krtolica that firewall adapter 24A sends communication requests which are received at Media Server 20M.

We are not persuaded by Patent Owner's argument that Krtolica's firewall adapters and media server do not exchange communication requests because they are "passive" devices. *See* PO Resp. 25. Patent Owner relies on the testimony of Dr. Jeffay, who states that "[t]he firewall adapters and

Media Server in Krtolica are passive devices," which "operate on traffic that transits them but do not directly communicate with each other." Ex. 2009 ¶¶ 106–107. It is unclear, however, what Dr. Jeffay means by the term "passive device," which is not used in claim 1, or why Krtolica's media server is such a "passive device." And, even if the media server was "passive," Dr. Jeffay fails to sufficiently explain why that would be inconsistent with it receiving a "communication request," as required by limitation 1[c]. Similarly, it is unclear what Dr. Jeffay means by "directly communicate" (which also does not appear in claim 1), particularly because it is clear that Krtolica's firewall adapter and media server do communicate with each other.

Dr. Jeffay also fails to convincingly explain why Krtolica's Media Server 20M does not receive "communication requests" when it receives packets from the firewall adapter and "provid[es] communication functions such as NAT" to route the packets to another end user via firewall adapter 24B. *See* Ex. 1004, 4:26–28. Dr. Jeffay asserts that "NAT is a transparent connection-less process" in which "[n]o connection is established and no channel is opened," because "application endpoints communicating via a NAT device cannot tell that their traffic is NATed or that a NAT box is present" and "[a]pplication endpoints have no interaction at all with the NAT device." Ex. 2009 ¶ 107. Dr. Jeffay, however, does not explain why the endpoints must know that NAT is being used in order for a "communication request" to be received by the media server or for a communication channel to be established between the firewall adapter and the media server. To the contrary, we find more credible the testimony of Dr. Lavian that the media server receives a communication request when it receives packets from firewall adapter 24A as part of setting up a communication to endpoint 22B. *See* Ex. 1042 ¶ 4.

We are also not persuaded by Dr. Jeffay's assertion that "Dr. Lavian does not identify any specific request that is sent or received," and that "the word 'request' appears nowhere in Krtolica." *Id.* ¶ 108. As discussed above, Dr. Lavian presented persuasive evidence that a person of ordinary skill would understand that Krtolica's media server receives a "communication request." Given this showing, it is not necessary that Krtolica use the specific term "request" or expressly describe a specific request. *Cf. Whitserve, LLC v. Comput. Packages, Inc.*, 694 F.3d 10, 21 (Fed. Cir. 2012) (quoting *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009)). We also do not find convincing Dr. Jeffay's argument that Dr. Lavian's understanding of Krtolica "would render [claim 1[c]][10] meaningless as it would be satisfied in every network." Ex. 2009 ¶ 1009. Dr. Jeffay provides no evidence or analysis to back up this assertion. And, even if Dr. Jeffay was correct, consistent with our discussion of the claim language above, there is nothing preventing the claim from including routine network functions as limitations.

Finally, we do not agree with Patent Owner's argument that "a POSA would have understood the claimed communication request to be used '[i]n establishing the communication configuration in one of the communities/ sub-communities,' . . . not for establishing communication between endpoint devices (*i.e.* communication stations 26A and 26B), as Petitioner contends." *See* PO Sur-reply 1–2. For support, Patent Owner cites column 5, lines 20–

[10] Dr. Jeffay's declaration refers to 1[a], but this appears to be an error because claim limitation 1[c] is referenced in the heading of this section of Dr. Jeffay's declaration. *See* Ex. 2009 § VIII.A.Claim 1[c].

23 of the ’828 patent, which states that “[i]n establishing the communication configuration in one of the communities/sub-communities, a communication request is received at an external controller from a first controller behind a firewall.” Ex. 1001, 5:20–23. This statement, however, does not say that the “communication request” is not used “for establishing communication between endpoint devices,” as Patent Owner contends. Patent Owner also relies for support on page 80, lines 18–21 of Dr. Lavian’s deposition, but there, Dr. Lavian merely stated that sending a data packet may be a communication request in some cases but not all. Ex. 2025, 80:18–21. Thus, Patent Owner’s evidence does not support its interpretation of limitation 1[c].

Patent Owner further argues that “Dr. Lavian . . . admits that the information packets disclosed in Krtolica may not even contain ‘communication requests,’ and thus, cannot form the basis for an inherent teaching.” PO Sur-reply 2–3 (citing Ex. 2025, 80:18–21). We do not agree with this argument. To begin with, Petitioner’s argument does not rely on inherency, but rather focuses on what one of ordinary skill would understand to be taught by the references under § 103. Moreover, as noted above, the cited portion of Dr. Lavian’s deposition does not specifically discuss the data packets of Krtolica, but rather merely states that, in general, data packets may be communication requests in some cases. *See* Ex. 2025, 80:18–21. Indeed, Patent Owner ignores Dr. Lavian’s subsequent testimony explaining that at least some of the data packets sent to Media Server 20M in Krtolica will include communication requests that are used by Media Server 20M to open a channel to firewall adapter 24B:

> [Q]: And my question is: ***Data packets that pass through the media server, is that the same as a communication request?***

> A: ***Yes.*** Some of the data packets will be the packet to sen[d] the communication between 24A -- between Communication Station 26A on the left to Communication Station 26B on the right. And as part of the communication, part of the process of establishing the connection they will use the Media Server 20M.
>
> Q: So are the data packets from Communication Station 26A addressed to the Media Server 20M directly?
>
> A: ***As part of the process of sending the communication between 22A, typically between the communication station on the left 26A to the Communication Station 26B, they will send [a] communication request and Media Server 20M will receive the information and will open the channel*** specifically, will open the tunnel to Media Server 20M to Communication Station 24B on the right side of Figure 2.
>
> Q: So I want to go back to the Communication Station 26A. There are data packets that are sent from Communication Station 26A. There are data packets that are sent from Communication Station 26A. And my question is: Are they sent to the media server in the sense that the data packets are specifically sent into the media server? Is that what Krtolica discloses?
>
> [A]: What Krtolica discloses is sending the information to start to send a connection with the Communication Station 22B on the right. By doing so, it will send the information in this case the 20B, the tunnel information between 26A on the left to the Media Server 20M, and the media server will know where is the exact location and all the information related to Communication Station 26B, and it will open the connection and will make the routing between both of those. That's the purpose of media server.
>
> Q: I'm trying to be more specific than that. ***So you're saying that the data packets from Communication Station 26A, they send a communication request directed to 26B, correct?***
>
> A: ***Yes.***

Ex. 2025, 81:3–24 (objections omitted).

Based on the above evidence, including the ’828 patent, the disclosures of Krtolica, and an assessment of the credibility of Dr. Lavian and Dr. Jeffay, we find that Petitioner has shown by a preponderance of the evidence that limitation 1[c] is taught by Krtolica.

e. Limitation 1[d]: “establishing a communication channel between said controller and said external controller”

Petitioner contends that Krtolica teaches establishing a communication channel carrying information data packets from firewall adapter 24A (the first controller) and media server 20M (the external controller). Pet. 40 (citing Ex. 1004, 4:11–16, Fig. 2). Petitioner also contends that the data packets are tunneled by the firewall adapter onto a single port containing multiple corresponding logical channels. *Id.* (citing Ex. 1004, 5:7–26).

Patent Owner does not specifically address Petitioner’s showing as to limitation 1[d]. Based on the entirety of the record, we find that Petitioner has shown, by a preponderance of the evidence, that Krtolica teaches this limitation.

f. Limitation 1[e]: “opening a second communication channel between said external controller and at least one other controller behind another firewall, wherein said at least one other controller is configured to service a single endpoint communication device”

Petitioner contends that Krtolica discloses a second communication channel between an external controller (media server 20M) and at least one other controller (firewall adapter 24B) behind another firewall (firewall 25B). *Id.* at 41 (citing Ex. 1004, Fig. 2, 4:14–16). Petitioner also contends that the endpoint units of Krtolica (endpoint communication devices) may be simple PCs operated by individuals and therefore can be configured to service a single endpoint communication device. *Id.* at 42 (citing Ex. 1004, 4:1–2), As an example, Petitioner points to Figure 2 of Krtolica, which illustrates a single endpoint unit 22B communicatively coupled to firewall adapter 24B. *Id.*

Patent Owner does not specifically address Petitioner's showing as to limitation 1[e]. Based on the entirety of the record, we find that Petitioner has shown, by a preponderance of the evidence, that Krtolica teaches this limitation.

g. *Limitation 1[f]: "transmitting multimedia communication data between said controller and said at least one other controller wherein said multimedia communication data passes through said external controller"*

Petitioner contends that Krtolica discloses transmitting data packets (information data packets 20D) from one endpoint communication device (endpoint unit 22A) to another endpoint device (endpoint unit 22B). *Id.* at 42–43 (citing Ex. 1004, 4:11–12). Petitioner also contends that these data packets are transmitted through a first controller (firewall adapter 24A) to a second controller (firewall adapter 24B) and pass through an external controller (media server 20M). *Id.* (citing Ex. 1004, 4:11–16). Petitioner further contends that the information data packets of Krtolica comprise multimedia communication in the form of "voice and/or video data." *Id.* (citing Ex. 1004, 6:50–52).

Patent Owner does not specifically address Petitioner's showing as to limitation 1[f]. Based on the entirety of the record, we find that Petitioner has shown, by a preponderance of the evidence, that Krtolica teaches this limitation.

h. Limitation 1[g]: "distributing said multimedia communication data to one or more of said plurality of endpoint communication devices and said single endpoint communication device"

Petitioner contends that Krtolica's media server (the external controller) distributes multimedia communication data to the endpoint communication devices shown in Figure 2, including endpoint units 22A and 22B, along with two other unmarked endpoint units. Pet. 43–44. Petitioner further contends that Krtolica discloses that each of the endpoint units illustrated in Figure 2 may include one or more endpoint units. *Id.* at 44 (citing Ex. 1004, 4:1–6). For example, Petitioner asserts, the endpoint units "may be simple PCs operated by individuals at a single work station," "a collection of end user PCs," or "complex computer system(s) operated by large organizations." *Id.* (citing Ex. 1004, 4:1–6).

Patent Owner does not specifically address Petitioner's showing as to limitation 1[g]. Based on the entirety of the record, we find that Petitioner has shown, by a preponderance of the evidence, that Krtolica teaches this limitation.

i. Conclusion

In addition to the arguments considered above, we have also considered Patent Owner's arguments and evidence concerning objective indicia of obviousness, as discussed in detail in Section II.H below. For the reasons discussed, we find that Patent Owner's evidence purportedly showing long-felt need, unexpected results, and industry praise does not outweigh Petitioner's evidence concerning the obviousness of claim 1. On the full record, Petitioner has established by a preponderance of the evidence that claim 1 would have been obvious over Krtolica in view of Rosenberg.

4. Claim 3

Claim 3 depends from claim 1, and further recites the step of "transmitting a security key from said controller to said external controller for authorization of said communication request." Ex. 1001, 14:29–32. Petitioner relies on Rosenberg for this limitation, and argues that it would have been obvious to combine Rosenberg with Krtolica to teach the invention of claim 3. Pet. 44–47. Patent Owner argues that Rosenberg does not teach this limitation, and that Petitioner's rationale for the combination is deficient. We will first discuss whether the limitations of claim 3 are taught by Rosenberg, and then turn to motivation to combine Rosenberg with Krtolica.

a. Whether Rosenberg Teaches Claim 3

(1) The Arguments in the Petition

In arguing that Rosenberg discloses claim 3, Petitioner relies on Rosenberg's Figure 1, reproduced below:

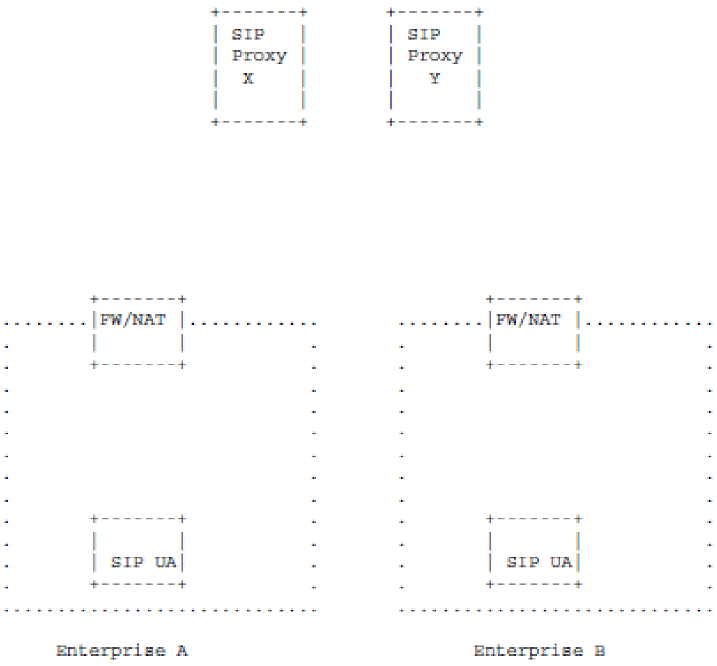


Figure 1: Network Architecture

As discussed in the section on Rosenberg above, Figure 1 shows Rosenberg's network architecture. *See* § II.D.2, *supra*; Ex. 1005, 2–3. Petitioner identifies the SIP UA as the claimed "controller" and the SIP Proxy X as the claimed "external controller." *Id.* Petitioner argues that "Rosenberg discloses 'originating request[s] from the caller [the SIP UA] through a firewall/NAT, out to a proxy.'" Pet. 45 (citing Ex. 1005, 4). According to Petitioner, the "originating request of Rosenberg (running over port 443) requires the calling device to 'negotiate a secure channel' for the connection" using transport layer security (TLS) and, "[o]nce [a] TLS connection is secured, the client can send SIP messages over the connection." *Id.* at 45–46 (citing Ex. 1005, 4).

Petitioner further argues, relying on the testimony of Dr. Lavian, that "[p]art of negotiating this secure channel includes transmission of security keys." Pet. 46 (citing Ex. 1002 ¶ 130). According to Petitioner, "Rosenberg explains that the ‘TLS server process (to receive RTP) embedded within a SIP enabled communications client’ . . . ‘require[s] a public/private key and its associated certificate available to the client.’” *Id.* (citations omitted) (citing Ex. 1005, 12). “Similarly,” Petitioner asserts, “use of a TLS client will require that the client be configured with the keys of well known CAs [Certification Authorities].” *Id.* (citing Ex. 1005, 12). “Thus,” Petitioner contends, “Rosenberg discloses transmission of a security key from the SIP UA to its proxy for authorization of the communication request.” *Id.* (citing Ex. 1002, ¶ 130).

Patent Owner makes three arguments in response, which will be discussed in turn below.

(2) Patent Owner’s argument that Rosenberg’s SIP UAs are not “controllers behind a firewall” as claimed

First, Patent Owner argues that Rosenberg does not include “a controller that is behind a firewall” and, therefore, cannot “transmit[] a security key from said controller to said external controller.” PO Resp. 26 (citing Ex. 2009 ¶¶ 112–120). According to Patent Owner, the only devices behind the firewall disclosed in Rosenberg are the SIP UAs, which a person of ordinary skill would have understood to be an “endpoint communication device,” not “a controller.” *Id.* (citing Ex. 2009 ¶¶ 112–120). Patent Owner further argues that the Petition and Dr. Lavian admitted that Rosenberg’s SIP UA is not a controller. *Id.* 28 (citing Pet. 51; Ex. 1002 ¶ 135); PO Sur-reply 5 (citing Ex. 2025, 84:19–86.6).

Petitioner responds that the SIP UA is a user agent that can comprise a controller and, in any event, the distinction between an endpoint device and a controller is immaterial because the SIP UA is performing the functionality associated with the controller in the ’828 patent, namely, transmitting a security key to an external controller for communication authorization. Pet. Reply 5 (citing Ex. 1042 ¶ 6). Petitioner also contests Patent Owner’s assertion that Petitioner and Dr. Lavian stated that the SIP UA is not a controller. *Id.* Finally, Petitioner argues that whether the UA is a controller is irrelevant because Petitioner is relying on Krtolica for the claimed “said controller” and “said external controller,” and relying on Rosenberg for its disclosure of the transmission of a security key. *Id.* (citing Pet. 45–46; Ex. 1005, 12).

We do not find Patent Owner’s arguments convincing. Petitioner relies on Krtolica’s firewall adapter 14S as the “controller that is behind a firewall,” which is introduced in claim 1, limitation 1[b]. Pet. 31–33. Petitioner relies on Rosenberg for claim 3’s requirement of transmission of a security key from the controller behind the firewall to the external controller. *Id.* at 44–47. Patent Owner does not argue that Krtolica’s firewall adapter 14 does not meet the “controller that is behind a firewall” limitation of claim 1[b] and, as discussed in Section II.D.3.b above, we find that Petitioner has made a sufficient showing that Krtolica discloses this claim limitation. Therefore, Petitioner need not show that this limitation is also present in Rosenberg. It is well-settled that “non-obviousness [cannot be established] by attacking references individually,” when, as here, the asserted ground of obviousness is based upon the combined teachings of Krtolica and Rosenberg. *In re Keller*, 642 F.2d 413, 426 (CCPA 1981) *see In re Merck & Co.*, Inc., 800 F.2d 1091, 1097 (Fed. Cir. 1986). Instead, the test is what the combined teachings of these references would have taught or suggested to one with ordinary skill in the art. *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991).

We also disagree with Patent Owner's assertion that Petitioner and Dr. Lavian admitted that Rosenberg's SIP UA is not a controller. To the contrary, Dr. Lavian testified that "the SIP UA [in Rosenberg] comprises the claimed controller." Ex. 1002 ¶ 128; *see* Ex. 1042 ¶ 6 ("The SIP UA in Rosenberg is a user agent that can comprise a controller."); Pet. 51 ("Rosenberg's UAs correspond to, *or are connected with*, endpoint communication devices." (emphasis added)). We find, based on Rosenberg's disclosure and Dr. Lavian's testimony, that Rosenberg's SIP UA acts as a "controller behind a firewall" because it is behind the firewall FW/NAT in Rosenberg's Figure 2 and controls communication through the firewall to the SIP Proxies. *See* Ex. 1002 ¶¶ 128–129 (explaining that "[t]he SIP UA comprises the claimed controller" and "'negotiate[s] a secure channel' for the connection," resulting in a "TLS connection" over which "the client can send SIP messages"); Ex. 1005, 4 (explaining that the SIP UA originates a request from the caller through a firewall out to a proxy, which requires the device to "negotiate a secure channel" for the connection).

(3) Patent Owner's argument that Rosenberg's SIP Proxies are not "external controllers" as claimed

Second, Patent Owner argues that Rosenberg's SIP Proxies do not constitute the claimed "external controller" because "multimedia communication data" does not pass through them, as claim 1[f] requires. PO Resp. 28 (citing Ex. 2009 ¶ 115). Patent Owner presents an annotated version of Rosenberg Figure 2 (PO Resp. 29), reproduced below, to illustrate this argument:

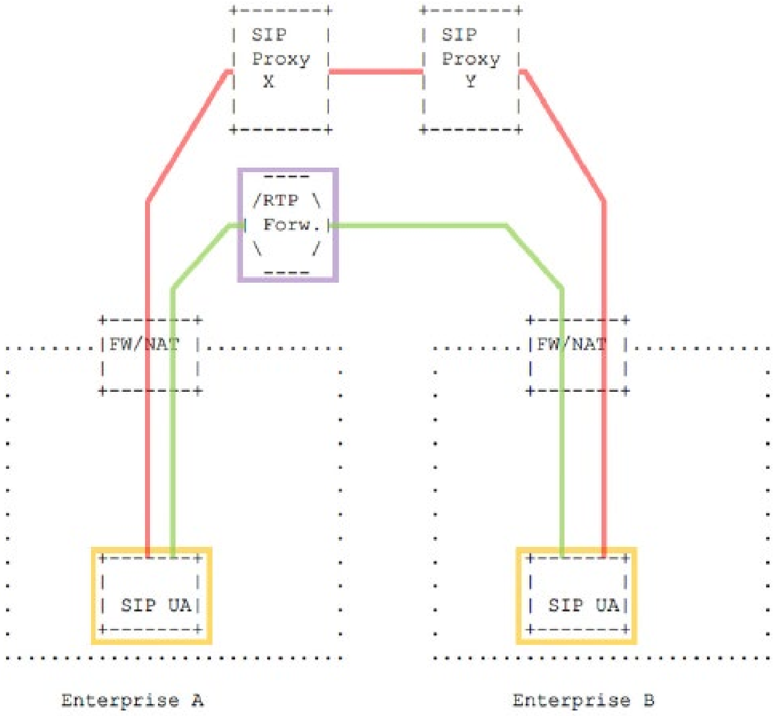


Figure 2: RTP Forwarders

Patent Owner's annotated version of Rosenberg's Figure 2 showing the paths taken by signaling and multimedia data.

In Patent Owner's annotated version of Rosenberg's Figure 2, above, SIP signaling (highlighted in red) passes through the SIP Proxies, with RTP traffic (highlighted in green) passing through the RTP forwarder (highlighted in purple). PO Resp. 28. Thus, Patent Owner argues, because the multimedia data is part of the RTP traffic, and the RTP traffic does not pass through the SIP Proxies, the SIP Proxies cannot be "external controllers" as required by claim 1. *Id.* at 28–29.

Petitioner responds that this argument is incorrect because it excludes embodiments in the '828 patent that are directed to SIP and H.323. Reply 6. According to Petitioner, SIP does not transmit the actual media, so when the '828 patent discusses a "SIP data packet" it is necessarily referring to SIP messaging packets that set up and control the RTP channel, not the actual payload. *Id.* (citing Ex. 1001, 3:19; Ex. 1042 ¶¶ 7–8). Additionally, Petitioner argues that the "external controller" language comes from claim 1[f], which Patent Owner does not dispute, and that the Petition relies on Krtolica to satisfy that limitation. *Id.*

We agree with Petitioner. To begin with, Petitioner relies on Krtolica's media server 20M as the "external controller" through which multimedia communication data passes, which is introduced in claim 1, limitation 1[c]. Pet. 43. Petitioner only relies on Rosenberg for claim 3's requirement for transmission of a security key from the controller behind the firewall to the external controller. *Id.* at 44–47. As discussed in Section II.D.3.d above, we find that Petitioner has made a sufficient showing that Krtolica discloses this claim limitation, including the "external controller." Therefore, Petitioner need not show that this limitation is also present in Rosenberg. *See In re Keller*, 642 F.2d 413, 426 (CCPA 1981) (Where obviousness is based on a combinations of references, one cannot show nonobviousness by attacking references individually.); *In re Merck & Co.*, Inc., 800 F.2d 1091, 1097 (Fed. Cir. 1986) (same).

Additionally, we are not persuaded by Patent Owner's argument that Rosenberg's SIP Proxies cannot constitute the claimed "external controller" because they do not handle "multimedia communication data," but instead only handle SIP signaling. *See* PO Resp. 28. As discussed in Section II.B above, we have construed "multimedia communication data" to encompass signaling data relating to multimedia communication. And, the '828 patent describes SIP as a multimedia communication protocol. *See* Ex. 1001, 2:59–67, 3:33–34, 7:27–35. Therefore, we find that Rosenberg's SIP Proxy X receives multimedia communication data from the SIP UA.

(4) Patent Owner's argument that Rosenberg does not transmit security keys between the SIP UA and SIP Proxy

Third, Patent Owner argues, citing Dr. Jeffay, that "the cited portions of *Rosenberg* on which [Petitioner and Dr. Lavian] rely, indicate[] that security keys are *not* transmitted between the SIP UA and SIP Proxy." PO Resp. 27 (citing Ex. 2009 ¶¶ 112–120). Rather, Patent Owner contends, "Rosenberg expressly teaches the exchange of a security key with a CA [Certification Authority] and not between the SIP UA and its SIP Proxy as Petitioner contends." PO Sur-reply 4.

We do not find Patent Owner's argument persuasive. Rosenberg discloses "originating request[s] from the caller [the SIP UA] through a firewall/NAT, out to a proxy," and that "the connection starts out with TLS" and "negotiates a secure channel" for the connection. Ex. 1005, 4. "Once the TLS connection is secured," Rosenberg explains, "the client can send SIP messages over this connection." *Id.* According to Rosenberg this "TLS server process"

> will require a public/private key and its associated certificate, available to the client, issued from a Certification Authority (CA) that is known to the other party. Similarly, use of a TLS client will require that the client be configured with the keys of a set of well known CAs.

Id. at 12.

We find that this disclosure of Rosenberg teaches: (1) the use of TLS between the SIP UA and SIP proxy X, and (2) that the use of TLS requires an exchange of a security key. From this disclosure, we find that one of ordinary skill would understand that a security key is exchanged between Rosenberg's SIP UA and SIP Proxy X. Our conclusion is reinforced by Dr. Lavian's testimony, which explains that "[p]art of negotiating this secure

[TLS] channel" between the SIP UA and the SIP Proxy X "includes transmission of security keys." Ex. 1002 ¶ 130. Additionally, Dr. Lavian further testifies that, in the above-referenced discussion from page 12 of Rosenberg, "Rosenberg discloses transmission of a security key from the SIP UA to its proxy for authorization of the communication request." *Id.* (citing Ex. 1005, 12). We find this testimony to be credible and consistent with Rosenberg's disclosure.

We are not persuaded by Patent Owner's argument that "Rosenberg expressly teaches the exchange of a security key with a CA [Certification Authority] and not between the SIP UA and its SIP Proxy as Petitioner contends." PO Sur-reply 4. We see nothing in Rosenberg that suggests that keys are not transmitted between the SIP UA and SIP Proxy, and Dr. Jeffay's testimony fails to provide sufficient explanation to support Patent Owner's argument in this regard. *See* Ex. 2009 ¶ 115 (alleging in conclusory fashion that Dr. Lavian's testimony "makes clear that to the extent any keys are transmitted, they are transmitted from a Certificate Authority and not from any SIP UA or 'SIP Proxy X'").[11]

Consequently, we find that Rosenberg discloses transmitting a security key from the SIP UA to the SIP Proxy X for authorization of a communication request.

b. Motivation to Combine Rosenberg and Krtolica

Petitioner argues that it would have been obvious to implement Rosenberg's security keys in Krtolica. Pet. 46–47. Petitioner asserts that

[11] Indeed, when asked during the hearing how the keys in Rosenberg would be exchanged if not between the SIP UA and SIP Proxy X, Patent Owner's counsel responded: "I don't know." Tr. 27:18–25.

both references are in the same field of endeavor—firewall traversal—and adding a security key to Krtolica would have been simply modifying known work in the same field in an entirely predictable manner. *Id.* Therefore, according to Petitioner, combining Rosenberg and Krtolica would have been the use of a known technique (use of security keys) to improve similar devices (the firewall traversal system of Krtolica) in the same way (to achieve a more secure network). *Id.* at 47. Petitioner further argues one of Krtolica's goals is maintaining high security in the network, and implementing security keys furthers this goal. *Id.* at 47 (citing Ex. 1004, 2:33–36).

Patent Owner argues that Petitioner's showing of motivation to combine is deficient because Petitioner fails to explain with particularity which elements of Krtolica would be modified or how they would be modified. PO Resp. 30–31. Relying on Dr. Jeffay, Patent Owner asserts that a person of ordinary skill "would have understood *Krtolica* and *Rosenberg* as disclosing *dissimilar* and *incompatible* architectures, such that *Rosenberg's* use of security keys (through its use of TLS functionality) could not simply be integrated into the firewall adapter or media server of *Krtolica*." *Id.* at 31 (citing Ex. 2009 ¶¶ 112–120, 172–177). Due to these alleged incompatibilities, Patent Owner argues that a person of ordinary skill would not have had a reasonable expectation of success in combining the references as proposed. *Id.* at 33. Patent Owner further argues that Petitioner and Dr. Lavian "fail to address the critical distinctions between maintaining network security and ensuring that communications are private (*i.e.*, through the use of encryption in TLS/SSL)," explaining that "*Krtolica* aims to maintain high network security, *i.e.*, by limiting the number of ports [to] be opened on a firewall, whereas *Rosenberg*'s use of TLS operates to secure *the connection* between the SIP UA and its associated SIP Proxy." *Id.* at 32.

We find that Petitioner has demonstrated a sufficient motivation to combine Rosenberg's use of security keys with Krtolica's system. To begin with, we agree with Dr. Lavian's testimony (which Patent Owner does not dispute) that security keys were well understood when Rosenberg was published in 2000, particularly because the TLS and SSL protocols (which use security keys) were originally published in the 1990s. *See* Ex. 1042 ¶ 9. We also agree with Petitioner and Dr. Lavian that Krtolica and Rosenberg are in the field of firewall traversal across networks (*see* Ex. 1004, Abstr; Ex. 1005, 1), and that Krtolica states that one of its goals is to "maintain[] high security" in the network (Ex. 1004, 2:33–36). Based on this evidence, we find that modifying Krtolica to use a security key as in Rosenberg would have been "the predictable use of prior art elements according to their established functions," and would have been no more than the "combination of familiar elements according to known methods" that "does no more than yield predictable results." *KSR*, 550 U.S. at 416–417.

We also agree with Dr. Lavian's testimony that it would have been obvious for a person of skill to modify Krtolica's firewall traversal using HTTP over port 80 by substituting Rosenberg's similar firewall traversal method using HTTPS over TLS/SSL port 443, which uses security keys. As Dr. Lavian explains, both methods were known at the time of the invention, and the modification is a simple substitution of one known element (HTTPS over port 443) for another known element (HTTP over port 80) to obtain predictable results (firewall traversal). Ex. 1002 ¶ 117. Based on the above testimony, we find that Petitioner has set forth with sufficient particularity how Krtolica would be modified in the proposed combination.

We are not persuaded by Patent Owner's argument that one of skill would not or could not have combined Krtolica and Rosenberg because they use "dissimilar and incompatible architectures." PO Resp. 31. As Dr. Jeffay points out, "Krtolica is a protocol agnostic system and seeks to support all voice/video/data communications." Ex. 2009 ¶ 173. And, as discussed above, the TLS protocol discussed in Rosenberg was well known. We agree with Dr. Lavian that one of ordinary skill could readily have implemented a protocol agnostic system like Krtolica using the well-known TLS protocol to increase security, with a reasonable expectation of success. *See* Ex. 1042 ¶¶ 10, 12.

Finally, we are not persuaded by Patent Owner's argument that Petitioner fails to address the distinction between maintaining privacy and network security, and that "[i]f anything, the use of TLS would undermine network security, as it would prevent the FW/NAT from examining data packets at the application layer in order to detect malicious traffic." PO Resp. 31–32. Dr. Lavian disagrees that TLS would undermine network security, and points out that TLS was "developed for the sole purpose of security network connections from prying by unauthorized parties." Ex. 1042 ¶ 11. "In fact," Dr. Lavian states, "a POSA would not consider a network secure unless it was using SSL or TLS when sending traffic across the Internet." *Id.* We find Dr. Lavian's testimony credible and thus, even if we were to accept Patent Owner's assertion that TLS could potentially interfere with the ability of the FW/NAT from examining data packets at the application layer, the benefits of TLS encryption would nonetheless motivate one of ordinary skill to use it in the system of Krtolica.

Consequently, we find that Petitioner has sufficiently established that one of ordinary skill in the art would have been motivated to combine

Krtolica and Rosenberg as Petitioner proposes, and would have had a reasonable expectation of success in doing so.

c. Conclusion as to Claim 3

In addition to the arguments considered above, we have also considered Patent Owner's arguments and evidence concerning objective indicia of obviousness, as discussed in detail in Section II.H below. For the reasons discussed, we find that Patent Owner's evidence purportedly showing long-felt need, unexpected results, and industry praise, does not outweigh Petitioner's evidence concerning the obviousness of claim 3. On the full record, Petitioner has established by a preponderance of the evidence that claim 3 would have been obvious over Krtolica in view of Rosenberg.

5. Claim 4

Claim 4 depends from claim 1, and further recites the step of "sending an external request from said external controller to an additional external controller responsive to said communication request requesting to communicate with an additional endpoint communication device connected to said additional external controller." Ex. 1001, 14:33–39. Petitioner relies on the combination of Krtolica and Rosenberg for this claim. Pet. 48–52. Petitioner states that this claim covers the addition of a second external controller for a second group of endpoint devices behind a second firewall, and argues that this is a "common network topology that a POSITA would have expected and understood." *Id.* at 48. Petitioner argues that although Krtolica's Figure 2 only explicitly shows one media server (corresponding to the external controller), Krtolica discloses that its system may contain multiple "media servers" spread out across the Internet. *Id.* at 49 (citing Ex. 1004, 4:26–28). According to Petitioner, a person of ordinary skill would have understood that Krtolica "could communicate over the Internet with the disclosed additional endpoints through additional media servers connected with those endpoints." *Id*. (citing Ex. 1002 ¶ 133).

Petitioner further asserts that, although Krtolica does not expressly state that its media servers send communication requests to each other, Rosenberg discloses two external controllers, SIP Proxy X and SIP Proxy Y, that send communication requests between them. *Id.* at 48–51. According to Petitioner, Rosenberg's Proxy X forwards a call to Proxy Y, which in turn forwards the call to endpoint communication devices. *Id.* at 50. Petitioner argues that it would have been obvious to combine the references because Krtolica suggests the use of additional external controllers across the Internet, and Rosenberg states that the claimed external controllers already exist on the Internet as part of typical network architecture. *Id.* at 51. According to Petitioner, such a combination would have merely been combining prior art elements according to known methods to yield predictable results. *Id.* at 52.

Patent Owner argues that Petitioner fails to explain with particularity how Rosenberg's additional external controller would be implemented in Krtolica's system. PO Resp. 35. For example, Patent Owner argues that it is unclear whether the combination would require a second media server (as in Krtolica), a SIP Proxy (as in Rosenberg), or something else, and what modifications would be required to Krtolica's media server. *Id.* at 35–36. Next, Patent Owner argues that Petitioner fails to explain why a second media server would be required in Krtolica beyond the single media server shown in Figure 2, or what in Rosenberg would motivate the addition of a second media server. *Id.* at 36. Third, Patent Owner argues that Krtolica's media server and Rosenberg's SIP proxy servers are fundamentally different devices, and that modifying Krtolica's media server to operate as a proxy server would require a substantial redesign of Krtolica with no apparent benefit. *Id.* at 37–38. For similar reasons, Patent Owner also argues that one of ordinary skill would not have had a reasonable expectation of success in combining Krtolica and Rosenberg to arrive at the claimed invention. *Id.* at 38.

We agree that Petitioner has sufficiently shown that claim 4 is taught by the combination of Krtolica and Rosenberg. First, we agree with Petitioner that Krtolica teaches the use of multiple media servers across the Internet. Specifically, Krtolica states that "[t]he internet may contain media servers for providing communication functions" and that a "media server may be accessed by hundreds of parties simultaneously, each of which may have a firewall with a firewall adapter." Ex. 1004, 4:26–34. Krtolica further explains that media servers frequently act as the "visible address" for private local area networks (LANs) that employ invisible private network addresses. *Id.* at 4:28–32; *see* Ex. 1002 ¶ 136. We credit Dr. Lavian's testimony that, based on this disclosure, a person of ordinary skill "would understand that the system of Krtolica could communicate over the Internet with the disclosed additional endpoints through additional media servers connected with those endpoints" and that, "[s]ince geographically remote LANs would each require a separate media server, a POSITA seeking to implement Krtolica between two such LANs would be motivated to include a second media server." Ex. 1002 ¶¶ 133, 136. In light of this evidence, we find that one of ordinary skill would have found it obvious based on Krtolica to use multiple media servers that can be geographically remote from each other and can each serve one or more endpoints.

Although Krtolica does not expressly state that the separate media servers can send communication requests to each other, we find that having them do so would have been obvious to a person of ordinary skill. As discussed above, we find that Krtolica teaches having one endpoint device send a request to Krtolica's media server to communicate with another endpoint device. *See* Section II.D.3.d, *supra.* In a system with two geographically distant media servers each serving their own endpoint(s), it would have been obvious to one of ordinary skill that the first media server that receives the request for communication with a geographically remote endpoint device would then request communication with a second media server that serves that remote endpoint device. In making this finding, we credit Dr. Lavian's testimony that the use of "two controllers outside of a firewall sending communication requests between them" was "a common arrangement that was widely known and widely implemented [in] [intranet and] Internet architectures long before and at the time of the invention," and that "[t]he ability for two controllers to communicate with one another is baked into the devices themselves and the protocols they run and would be well understood by a POSA." Ex. 1042 ¶ 15.

We also find that sending communication requests between two external controllers would have been obvious in view of Rosenberg. Rosenberg discloses sending a request from one external controller to another external controller requesting to communicate with an additional endpoint communication device connected to the additional external controller. Specifically, Rosenberg discloses SIP Proxy X and SIP Proxy Y, which are "external" controllers because they are external to the firewalls (the FW/NATs in Rosenberg's Figure 1). Ex. 1005, 2, Fig. 1. Rosenberg further discloses forwarding a call from SIP Proxy X (the first external controller) to SIP Proxy Y (the second external controller), and then to the called party (the additional endpoint device connected to the second endpoint controller). Ex. 1005, 2 ("The caller uses proxy X as its local outbound proxy, which forwards the call to the proxy of the called party, Y, also outside of the firewall. The call is then forwarded to the called party within enterprise B."). We agree with Petitioner that this call involves a request from one external controller to another external controller requesting to communicate with an additional endpoint communication device, as claimed.

We also find sufficient motivation to combine Krtolica's firewall traversal system with Rosenberg's teaching of external controllers that send communication requests to each other. As discussed above, Krtolica suggests the use of multiple media servers across the Internet. *See* Ex. 1004, 4:26–34. Dr. Lavian and Dr. Jeffay both agree that Krtolica is "protocol agnostic." Ex. 1042 ¶ 15; Ex. 2009 ¶ 15. We also credit Dr. Lavian's testimony that, because Krtolica is protocol agnostic, its media servers "could easily be configured as SIP proxies as disclosed in Rosenberg," and one of skill would be motivated to do so to achieve, for example, additional security between endpoints. Ex. 1042 ¶ 16; Ex. 1002 ¶¶ 136–137. Based on this testimony, we find that combining Krtolica's system with Rosenberg's sending of a communication request from one external controller to another would have been no more than combining known prior art elements (firewalls and multiple external controllers) according to known methods to yield predictable results (providing an additional intermediary between endpoints). *See KSR*, 550 U.S. at 417.

We are not persuaded by Patent Owner's argument that Petitioner fails to explain with particularity how Rosenberg's additional external controller would be implemented in Krtolica's system, i.e., whether the combination would use a second media server as in Krtolica or SIP proxies as in Rosenberg. PO Resp. 35. Petitioner explains that its combination relies on multiple media servers as in Krtolica because "Krtolica envisions multiple media servers (the external controllers) communicating with one another," and relies on Rosenberg "to the extent it is necessary to show a network topology where one external controller sends communication requests to an additional communication controller." Pet. Reply 12; *see* Pet. 48–49. We find that this is a sufficiently detailed description of the combination upon which Petitioner relies.

We also are not persuaded by Patent Owner's argument that "there is no explanation offered in the Petition (or by Dr. Lavian) why a *second* media server would be *required*" in Krtolica. PO Resp. 36. Petitioner need not show that Krtolica "requires" a second media server; rather, it is sufficient to show that Krtolica teaches that a second media server may be used. As discussed above, Krtolica includes such a disclosure. *See* Ex. 1004, 4:26–34; Ex. 1002 ¶ 136.

Additionally, we do not agree with Patent Owner's argument that, due to fundamental differences between Krtolica's media server and Rosenberg's SIP proxy servers, modifying Krtolica's media server to operate as a proxy server would require a substantial redesign of Krtolica with no apparent benefit. *Id.* at 37–38. As discussed above, Petitioner proposes a combination using two of Krtolica's media servers, and therefore there is no need to modify either of Krtolica's media servers to operate as a proxy server. Moreover, Patent Owner's argument that the servers are fundamentally different is based on the assertion that the "sole ascribed function" of Krtolica's media servers "is providing NAT" (Network Address

Translation). PO Resp. 37–38. Dr. Lavian, however, testifies that "[n]othing in Krtolica indicates that the media server cannot perform SIP proxy functions instead of, or in addition to, Network Address Translation." Ex. 1042 ¶ 17. We credit Dr. Lavian's testimony, which is consistent with the disclosure of Krtolica. We find that the evidence of record does not show that there are fundamental incompatibilities that would prevent the functions of SIP proxies (as in Rosenberg) from being used as part of Krtolica's media server. For similar reasons, we also agree with Dr. Lavian's testimony that a person of ordinary skill would have had a reasonable expectation of success in combining Krtolica and Rosenberg as Petitioner proposes. *See* Ex. 1042 ¶ 18.

Finally, Patent Owner argues that "Petitioner fails to address how the teachings of Krtolica and Rosenberg would result in 'sending an external request from said external controller to an additional external controller *responsive to said communication request*' as required by the claims." PO Sur-reply 12. Petitioner, however, argues that Rosenberg's initiation of a call from the caller to Proxy X is a "communication request" and "[t]he external request is Proxy X forwarding the call to Proxy Y" in response to the communication request. Pet. 50–51 (citing Ex. 1005, 2). We find that this argument by Petitioner sufficiently addresses the language of claim 4.

In addition to the arguments considered above, we have also considered Patent Owner's arguments and evidence concerning objective indicia of obviousness, as discussed in detail in Section II.H below. For the reasons discussed, we find that Patent Owner's evidence purportedly showing long-felt need, unexpected results, and industry praise, does not outweigh Petitioner's evidence concerning the obviousness of claim 4.

On the full record, Petitioner has established by a preponderance of the evidence that claim 4 would have been obvious over Krtolica in view of Rosenberg.

6. Claim 5

Claim 5 depends from claim 4, and further recites the following additional steps (with reference numbers and letters added for convenience):

> 5[a] establishing an external channel between said external controller and said additional external controller; and
>
> 5[b] forwarding said multimedia communication data to said additional external controller from said external controller; and
>
> 5[c] distributing said multimedia communication data to said additional endpoint communication device.

Ex. 1001, 14:39–46.

Petitioner argues that claim 5 is obvious over Krtolica in view of Rosenberg. As to limitations 5[a] and 5[b], Petitioner argues that Rosenberg discloses establishing an external communication channel between a first external controller (SIP Proxy X) and a second external controller (SIP Proxy Y), and then forwarding multimedia communication data from the first external controller to the second external controller. Pet. 52–54 (citing Ex. 1005, 2, 11). As to limitation 5[c], Petitioner argues that Krtolica discloses distributing multimedia communication data to additional endpoint devices. *Id.* at 55 (citing Ex. 1004, Fig. 2 (showing four endpoint units), 4:1–4). To the extent one were to determine that Krtolica does not disclose limitation 5[c], Petitioner asserts that Rosenberg discloses distributing multimedia communication data to an additional endpoint communication device. *Id.* (citing Ex. 1005, 4, 11). Petitioner further argues that motivation exists for one of ordinary skill to make its proposed combination of Krtolica and Rosenberg. *Id.* at 52–56.

Patent Owner argues that Rosenberg's proxies cannot constitute the claimed "external controller" or "additional external controller" because "multimedia communication data" is not exchanged therebetween. PO Resp. 39. Patent Owner further argues that Rosenberg's RTP forwarder cannot be the claimed "external controller" or "additional external controller" because it routes media directly between the endpoints, not between the external controllers. *Id.* at 39–40.

We find that Petitioner has established that the limitations of claim 5 are met by the combination of Krtolica and Rosenberg. We are not persuaded by Patent Owner's argument because, as discussed above, we interpret the term "multimedia communication data" to encompass signaling data for multimedia communication. *See* Section II.A, *supra*. Therefore, we find the data exchanged between Rosenberg's SIP Proxy X and SIP Proxy Y to be "multimedia communication data," and these proxies qualify as "external controllers" as claimed.

In addition to the arguments considered above, we have also considered Patent Owner's arguments and evidence concerning objective indicia of obviousness, as discussed in detail in Section II.H below. For the reasons discussed, we find that Patent Owner's evidence purportedly showing long-felt need, unexpected results, and industry praise, does not outweigh Petitioner's evidence concerning the obviousness of claim 5.

On the full record, Petitioner has established by a preponderance of the evidence that claim 5 would have been obvious over Krtolica in view of Rosenberg.

7. Claims 9, 10, 11, 13, 14, 16, 17, 22, and 23

Patent Owner does not separately dispute Petitioner's basis for claims 9, 10, 11, 13, 14, 16, 17, 22, and 23. Petitioner's arguments for these claims are summarized below.

Claims 9 is dependent on claim 1, and recites "transmitting from said controller said plurality of single-port packets over a commonly-open port to said at least one other controller, said plurality of single-port packets traversing one or more firewalls using said commonly open port." Ex. 1001, 15:1–8. For this claim, Petitioner relies on its arguments for claim 1[b]. Petitioner further argues that Krtolica transmits single-port packets using a port that it identifies as "commonly-open" (network port 45P, which is typically port 80). Pet. 57 (citing Ex. 1004, 5:19–21, 5:47–48, 6:22–26, Fig. 5). Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 9 by a preponderance of the evidence.

Claim 10 is dependent on claim 9, and recites the following additional steps:

> receiving said plurality of single-port packets at said at least one other controller;
>
> reconverting, by said at least one other controller, said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets; and
>
> delivering, from said at least one other controller to said single endpoint communication device, said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol.

Ex. 1001, 15:9–20.

Petitioner argues that Krtolica discloses that the receive firewall adapter (the other controller) receives the plurality of single-port packets transmitted by the send firewall adapter, reconverts them to multiport packets, and delivers the multiport packets through multiple ports to the endpoint communication device (Krtolica's receive endpoint unit). Pet. 57–58 (citing Ex. 1004, 3:55–58, 5:1–3, 5:21–26, 5:36–38, 6:48–7:20, Figs. 1–4). Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 10 by a preponderance of the evidence.

Claim 11 is independent and is similar to claim 1. Ex. 1001, 15:21–48. Petitioner relies on the same evidence as for claim 1. Pet. 58–60. Petitioner further argues that the claimed "shared controllers" are Krtolica's firewall adapters, which may receive multiport packets from one or more endpoint units (the endpoint communication devices). *Id.* at 58. Petitioner further contends that Krtolica's endpoint units may either be a single device or a collection of devices. *Id.* (citing Ex. 1004, 4:1–6). Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 11 by a preponderance of the evidence.

Claim 13 is dependent on claim 11, and further recites "a security key repository within each of said one or more shared controllers and said individual controller, wherein said one or more shared controllers and said individual controller transmit a security key for verification by said external controller for each communication request issued to said external controller." Ex. 1001, 15:55–62. Petitioner points to its argument for claim 3 that Rosenberg discloses the transmission of security keys for verification by external controllers for each communication requests issued to the external controller. Pet. 60–61. Petitioner contends that both the client and server (corresponding to the shared and individual controller) are configured with security keys, which are maintained on the client and server by being saved in a repository. *Id.* at 61 (citing Ex. 1005, 2; 1002 ¶ 153). Petitioner further argues that it would have been obvious to combine Krtolica and Rosenberg for the reasons discussed for claim 3. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 13 by a preponderance of the evidence.

Claim 14 is dependent on claim 11 and recites "an external communication interface within said external controller for communicating with a second communication community." Ex. 1001, 15:63–67. Petitioner argues that Krtolica's media server is the external controller and contains an interface for communicating with other communication communities on the Internet. Pet. 61 (citing Ex. 1004, 5:30–32). Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 14 by a preponderance of the evidence.

Claim 16 is dependent on claim 11 and further recites that the one or more shared controllers and the at least one individual controller each comprise a device. Ex. 1001, 16:5–7. Petitioner argues that Krtolica's firewall adapters comprise shared and individual controllers, and are devices. Pet. 62 (citing Ex. 1004, 2:5–8). Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 16 by a preponderance of the evidence.

Claim 17 is independent and similar to claims 1 and 11. Ex. 1001, 16:8–59. Petitioner relies on its arguments for claims 1 and 4, and further argues that Krtolica's send endpoint units comprise local communication devices such as PCs or workstations, and that these devices initiate communication requests in the form of information data packets sent from one endpoint to another. Pet. 62–63 (citing Ex. 1004, 4:11–12). Petitioner argues that Krtolica's media servers comprise a second external controller, and Krtolica also discloses a remote communication device and second internal controller. Pet. 63. Petitioner points to Krtolica's Figure 2, which shows receive endpoint unit 22B, which is connected to receive firewall adapter 24B and, through firewall 25B, is connected to media server 20M. *Id.* (citing Ex. 1004, Fig. 2, 4:11–16). Petitioner further argues that it would have been obvious that Krtolica's system could communicate over the Internet with the disclosed additional endpoints through additional media servers connected with those endpoints, and that these additional endpoints could initiate communication requests. *Id.* at 63–64.

Petitioner additionally argues that Rosenberg teaches establishing a second communication connection between proxy server Y (the second external controller) and the SIP UA of Enterprise B (the second internal controller), and a third communication between the first external communication controller (SIP Proxy X) and the second external communication controller (SIP Proxy Y). *Id.* at 64–66. Petitioner further argues that it would have been obvious to combine these teachings of Rosenberg with Krtolica. *Id.* at 63–68. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 17 by a preponderance of the evidence.

Claim 22 is dependent on claim 17 and recites that "said first internal controller comprises said first intermediate communication device" and "said second internal controller comprises said second intermediate communication device." Ex. 1001, 18:7–10. Petitioner argues that Krtolica's send firewall adapters (the first internal controllers) comprise intermediate communication devices and Krtolica's receive firewall adapters comprise communication devices. Pet. 69–70. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 22 by a preponderance of the evidence.

Claim 23 is dependent on claim 17 and recites that "said transmitting, through the third communication connection, said plurality of single-port packets to a second intermediate communication device that is behind said second firewall comprises: transmitting said plurality of single-port packets over a commonly-open port." Ex. 1001, 18:11–16. Petitioner relies on its argument for claims 9 and 17. Pet. 70. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica and Rosenberg teaches claim 23 by a preponderance of the evidence.

E. Ground 2: Obviousness over Krtolica, Rosenberg, and Eisenberg — Claims 2, 12, 18, and 19

Petitioner contends that claims 2, 12, 18, and 19 are unpatentable as obvious under 35 U.S.C. § 103(a) over Krtolica, Rosenberg, and Eisenberg. Pet. 71–76. For the reasons that follow, Petitioner has demonstrated by a preponderance of the evidence that claims 2, 12, 18, and 19 are unpatentable on this ground.

1. Overview of Eisenberg

Eisenberg is directed to a method for traversing firewalls by tunneling through commonly open ports such as HTTPS port 443. Ex. 1006, code (57), 9:34–36. The basic configuration of Eisenberg's system is shown in Figure 7, reproduced below:

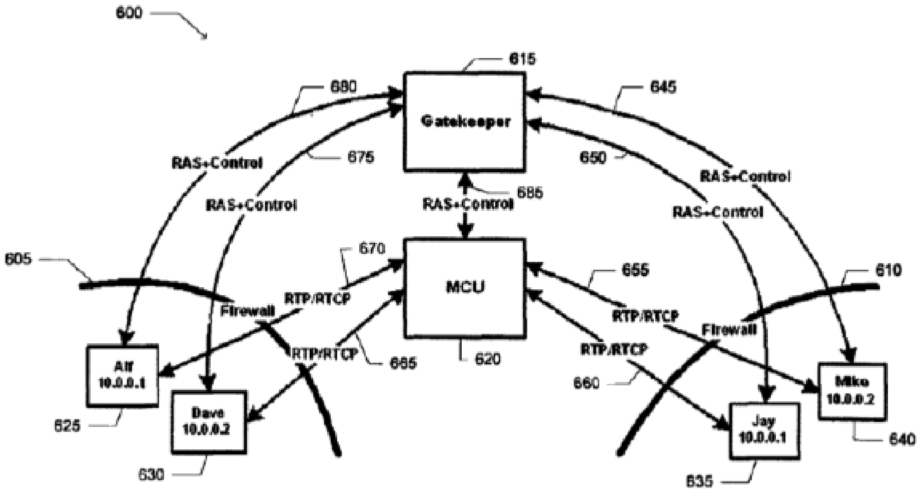


Fig. 7

Figure 7 shows Eisenberg's basic system, including firewalls 605 and 610 configured so that only outgoing TCP connections are allowed. Ex. 1006, 15:23–25. Endpoints 625–640, gatekeeper 615, and MCU 620 each have tunnel plugins installed to allow communications through the firewall. *Id.* at 15:25–27. Eisenberg also discloses the use of network security features such as authentication and encryption on the proxies to achieve secure connections. *Id.* at 1:67–2:4, 2:12–15.

2. Claim 2

Claim 2 depends from claim 1, and further recites the step of "verifying said communication request at said external controller." Ex. 1001, 16:26–28. The parties dispute: (1) whether Eisenberg discloses this limitation and (2) whether Petitioner has established sufficient motivation to combine Eisenberg with Krtolica and Rosenberg. These issues are discussed below.

a. Whether Eisenberg Teaches Claim 2

Petitioner argues that Eisenberg discloses the process of verifying communication requests at an external controller by, for example, using a typical NAT (network address translation) technique as a process to "qualify or authenticate the [communication] request." Pet. 71 (citing Ex. 1006, 1:67–2:4). Petitioner further points to Eisenberg's disclosure that proxies (i.e., external controllers) "may require authentication and/or encryption to achieve secure connections." *Id.* at 71–72 (citing Ex. 1006, 2:11–15). Petitioner argues that authentication and verification are performed as part of the same task and, therefore, the act of authentication includes verification. Pet. Reply 17 (citing Ex. 1002 ¶ 174; Ex. 1042 ¶¶ 19–21); *see also* Pet. 71–72 (citing Ex. 1002 ¶ 174).

Patent Owner acknowledges that "*Eisenberg* discloses a generic teaching of *authentication* performed by proxies and firewalls employing NAT." PO Resp. 43 (citing Ex. 1006, 1:65–2:4, 2:13–15). Patent Owner, however, argues that "a POSA would have understood that the claimed verification is a separate operation from authentication, and is performed for a distinct purpose—verification seeks to ensure that a request is valid, while authentication seeks to ensure that the device transmitting the request is authorized." *Id.* at 43–44 (citing Ex. 2009 ¶¶ 178–185). Patent Owner also argues that the '828 patent makes clear that "authenticating" and "verifying" are two independent steps. *Id.* at 44 (citing Ex. 1001, 10:29–31, 11:27–30).

We agree with Petitioner that, as used in the ’828 patent, authentication and verification are part of the same task, and that this task includes verifying the identity of a person or device making a particular communication request. For example, the ’828 patent states that “[a] communication channel is established between the first controller and the external controller after the external controller has *authenticated or verified the identification of the first controller*.” Ex. 1001, 5:25–28 (emphasis added). Similarly, the ’828 patent explains that “[w]hen front end controller 410 receives the request and the key, it first *verifies and authenticates* the key *to make sure that the component requesting access is a valid and authorized component*.” *Id.* at 10:28–31. *See also id.* at 5:54–55 (“Once everything is verified, a communication channel is open between the other endpoint and the other external controller.”), 7:16–18 (“[O]nce registered, various individuals may use backend 420 to establish verified connections into communication community 40 from remote, temporary locations.”). We also credit Dr. Lavian’s testimony that one of skill in the art would understand that “[a]uthentication is a process of verifying the identity of the other side” and that “the step of authentication in TLS or SSL would require verification.” Ex. 1042 ¶¶ 19–20 (footnote omitted).

We are not persuaded by Patent Owner’s argument that “verification” cannot include “authentication” because they are separate and distinct steps. *See* PO Resp. 43–44. Patent Owner points to the portions of the ’828 patent stating that the system “verifies and authenticates” a security key. *Id.* at 44 (citing Ex. 1001, 10:29–31, 11:27–30). The cited portions of the Specification, however, use the terms “verification” and “authentication” together to describe elements of the same task, *i.e.*, determining whether the component requesting access is authorized. *See* Ex. 1001, 10:29–31

("[F]ront end controller 410 . . . first verifies and authenticates the key to make sure that the component requesting access is a valid and authorized component."), 11:27–30 ("After verifying and authenticating the security key . . . , front end controller opens a communication channel."). Patent Owner has not directed us to anything in the '828 patent that describes "verification" as distinct from and not included as part of "authentication."

We further agree with Petitioner that Eisenberg discloses the process of verifying communication requests by an external controller through authentication. *See* Ex. 1006, 1:67–2:4 (disclosing that one typical NAT technique is a process to "qualify or authenticate the [communication] request"), 2:11–15 (explaining that proxies "act as the only path out from a private network to the public domain" and "may require authentication and/or encryption to achieve secure connections"), 9:52–53 (describing establishing an encrypted HTTPS tunnel over port 443, in which "the layers at which certain communication features are performed such as partner identification, user authentication"). We also agree with Dr. Lavian that one of ordinary skill would have understood this "authentication" process to include verifying the communication request to determine that it is valid, including as part of standard TLS/SSL handshake steps used in both Eisenberg and the '828 patent. *See* Ex. 1042 ¶¶ 19–22.

b. *Motivation to Combine Eisenberg With Krtolica and Rosenberg*

Petitioner argues that it would have been obvious to combine Eisenberg's teachings regarding verification with Krtolica's teachings regarding firewall traversal with a reasonable expectation of success. Pet. 72. Petitioner asserts that verification was well-known in the prior art, and therefore, it is merely combining a known technique (verification) with a known method (firewall traversal) to yield predictable results (enhanced security). *Id.* Petitioner further argues that Krtolica provides motivation for the use of verification because one of its primary objectives is implementing firewall traversal while maintaining or increasing network security, which would have motivated one of ordinary skill to look to Eisenberg's teachings regarding authentication. *Id.* (citing Ex. 1004, 1:7–10). Patent Owner argues that Petitioner's rationale is conclusory and provides no factual analysis to explain how introducing verification into the system of Krtolica would result in increased or enhanced network security such that a person of ordinary skill would have looked to incorporate the teachings of Eisenberg. PO Resp. 44–45.

We find that Petitioner has provided a sufficient motivation to make the proposed combination. As discussed above, Eisenberg teaches verification of a communication request for increasing security, and such verification techniques were well known in systems such as TLS/SSL. *See* Ex. 1042 ¶¶ 19–22. As the Supreme Court has explained, "if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *KSR*, 550 U.S. 417. We find that modifying Krtolica to use known verification techniques as in Rosenberg would have been within the level of ordinary skill, and would have been no more than the "combination of familiar elements according to known methods" that "does no more than yield predictable results." *See id*. at 416–417.

c. Conclusion as to Claim 2

In addition to the arguments considered above, we have also considered Patent Owner's arguments and evidence concerning objective indicia of obviousness, as discussed in detail in Section II.H below. For the reasons discussed, we find that Patent Owner's evidence purportedly showing long-felt need, unexpected results, and industry praise, does not outweigh Petitioner's evidence concerning the obviousness of claim 2. On the full record, Petitioner has established by a preponderance of the evidence that claim 2 would have been obvious over Krtolica, Rosenberg, and Eisenberg.

3. Claims 12, 18, and 19

Patent Owner does not separately dispute Petitioner's basis for claims 12, 18, and 19. Petitioner's arguments for these claims are summarized below.

Claims 12 is dependent on claim 11 and further recites "a verification utility within said external controller for verifying one or more communication requests from one or more of said one or more shared controllers and said individual controller." Ex. 1001, 15:49–54. Petitioner relies on the arguments presented for claims 2 and 11 above. Pet. 73. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, and Eisenberg teaches claim 12 by a preponderance of the evidence.

Claim 18 is dependent on claim 17, and further recites: (1) "verifying at said first external controller said first communication request prior to establishing said first communication connection"; and (2) "verifying at said second external controller said second communication request prior to said establishing said second communication connection." Ex. 1001, 16:60–66. Petitioner relies on its arguments for claims 2 and 17 above, and further asserts that the verification (authentication) occurs prior to establishing the first communication connection because it is necessary to achieve a secure connection. Pet. 73–74 (citing Ex. 1006, 2:12–15; Ex. 1002 ¶ 177). Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, and Eisenberg teaches claim 18 by a preponderance of the evidence.

Claim 19 is dependent on claim 18 and further recites "issuing a third communication request between said first and said external controllers" and "verifying said third communication request prior to said establishing said third communication connection." Ex. 1001, 16:67–17:4. Petitioner relies on its arguments for claims 2, 17, and 18 above. Pet. 75–76. Petitioner further argues that sending a third communication request between a first and second external controller, as required by claim 19, is equivalent to claim 4's recitation of "sending an external request from said external controller to an additional external controller," and as a result, Petitioner relies on its arguments discussed above for claim 4 for that limitation. Pet. 75. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, and Eisenberg teaches claim 19 by a preponderance of the evidence.

F. Ground 3: Obviousness over Krtolica, Rosenberg, and DSDP — Claims 6–8, 15, and 20

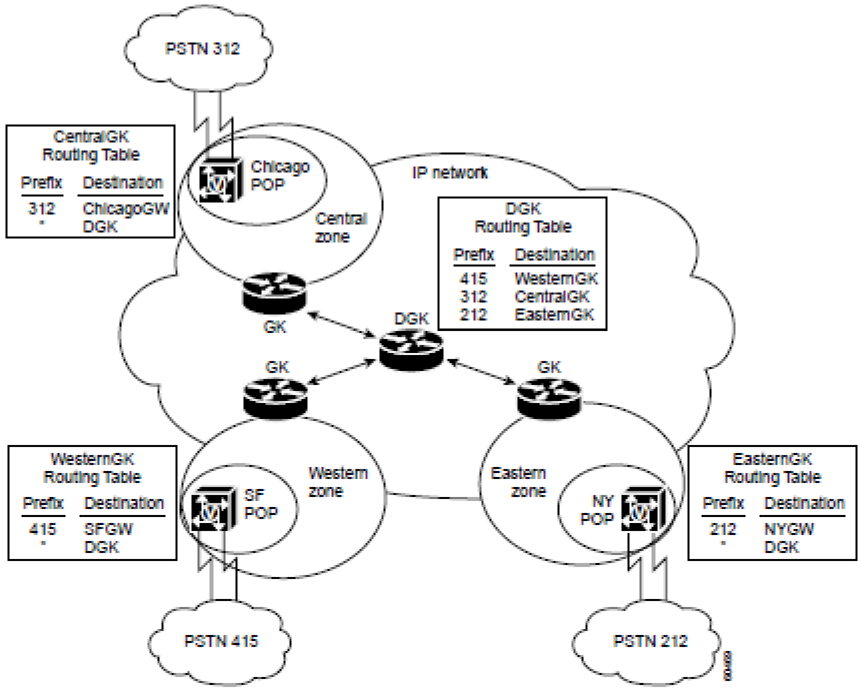
Petitioner contends that claims 6–8, 15, and 20 are unpatentable as obvious under 35 U.S.C. § 103(a) over Krtolica, Rosenberg, and DSDP. Pet. 76–82. For the reasons that follow, Petitioner has demonstrated by a preponderance of the evidence that claims 6–8, 15, and 20 are unpatentable on this ground.

1. Overview of DSDP[12]

DSDP describes how to design and implement static H.323 dial plans and how to configure and manage static H.323 dial plans on gateway and gatekeeper platforms for large VoIP networks. Ex. 1007, 1. DSDP explains that large VoIP networks may include multiple gatekeepers (GKs) that segment the network into various local zones, and a directory gatekeeper (DGK) to handle call routing between local GKs. *Id.* at 2–3. Figure 15 of DSDP, depicted below, shows a VoIP network architecture with multiple gatekeepers (GKs) and a directory gatekeeper (DGK).

[12] In the Preliminary Response, Patent Owner disputed the authenticity and printed publication status of DSDP. Prelim. Resp. 36–39, 50–53. No arguments on this issue were presented in the Patent Owner Response. *See generally* PO Resp. We ordered that "any arguments for patentability not raised in the [Patent Owner] response may be deemed waived," and we deem any arguments not raised in the Response to be waived by Patent Owner. Paper 20, 8.

Figure 15 Addition of a Directory Gatekeeper



DSDP's Figure 15 shows a VOIP architecture with multiple Gatekeepers (GKs) and a Directory Gatekeeper (DGK). Ex. 1007, 30–31.

2. Claim 6

Claim 6 depends from claim 1, and further recites the following steps (with reference numbers and letters added for convenience):

> 6[a] issuing a central request from said external controller to a central controller responsive to said communication request requesting to communicate with an external endpoint device not connected to one or more of said controller and said at least one other controller; and
>
> 6[b] receiving said multimedia communication data at said central controller.

Ex. 1001, 14:47–54.

According to Petitioner, claim 6 adds communications with a central controller to the communication system described in claim 1. Pet. 77. Petitioner argues that DSPD discloses a plurality of external controllers (gatekeepers or GKs) and central controllers (directory gatekeepers or DGKs). *Id.* Petitioner contends that the GKs "communicate with each other to route calls between GWs [gateways] located in different zones," and the DGKs "handle call routing between local GKs." *Id.* (quoting Ex. 1007, 2). According to Petitioner, when the GK determines that an endpoint is not connected to the GK, it may forward a central request through the DGK (the "central controller") asking to establish a call with the remote endpoint. *Id.* at 80. Petitioner argues that it would have been obvious to implement DSDP's basic architecture including a central controller (the DGK) with Krtolica's firewall traversal system in order to allow Krtolica's system to be able to communicate with geographically remote devices. *Id.* at 80–81.

Patent Owner argues that DSDP fails to disclose or suggest the step of "receiving said multimedia communication data at said central controller" because DSDP's DGKs do not receive "multimedia communication data." PO Resp. 46. Similar to claim 3, Petitioner argues that the actual media stream associated with the call is not routed through the GKs or DGKs, but rather is routed in an RTP media stream from one gateway to another. *Id.* at 46–48.

We agree with Petitioner's argument, and are not persuaded by Patent Owner's argument, for reasons similar to those discussed above with respect to claim 3. *See* § II.D.4(3). As discussed in Section II.B above, we have construed "multimedia communication data" to encompass signaling data relating to multimedia communication. And, the '828 patent describes H.323 as a multimedia communication protocol. *See* Ex. 1001, 2:57–65, 3:33–34, 7:27–35. We find that DSDP discloses routing H.323 control signaling through the DGK as follows:

> If the call is sent into the H.323 VoIP network, the GW then asks the gatekeeper to select the best endpoint to receive the call. Based on its routing table, the gatekeeper might find that this endpoint is a device within its own local zone of control

> and supply the IP address of the terminating endpoint. ***Alternatively, it might determine that the endpoint resides under the control of another remote gatekeeper. In this latter case, the gatekeeper would forward the location request (LRQ) to the remote gatekeeper either directly or through a directory gatekeeper.*** The remote gatekeeper would ultimately respond with the address of the terminating endpoint.

Ex. 1007, 4 (emphasis added). We find that this LRQ and other H.323 control information forwarded through a DKG constitutes "multimedia communication data." Therefore, we find that DSDP's DKG is a "central controller" that receives multimedia communication data from an "external controller" as recited in claim 6.

We also disagree with Patent Owner's assertion that Petitioner fails to provide a cogent explanation as to why or how a person of ordinary skill would have further modified the system of Krtolica to include a central controller as in DSDP. PO Resp. 48–50. Relying on testimony from Dr. Lavian, Petitioner argues that DSDP and Krtolica are in the same field of endeavor (multimedia (VoIP) networking), and that DSDP focuses on H.323 network architecture, which Krtolica identifies as one of the "three major standard ITU (international telecommunication union) configurations." Pet. 80–81 (quoting Ex. 104, 1:45–47; citing Ex. 1002 ¶¶ 80, 104, 177). Petitioner further argues that one of ordinary skill implementing Krtolica "would naturally have wanted the system to be able to communicate with geographically remote devices, and incorporating a central controller in the network disclosed by Krtolica was an obvious solution to this problem." *Id.* at 81 (citing Ex. 1002 ¶ 184). Thus, Petitioner explains, "implementing the architecture disclosed in DSDP would have been a variation that was predictable to a POSITA." *Id.*

Petitioner further asserts that DSDP's architecture (a central controller coordinating routing between remote locations) was a known architecture at the time of the invention, and implementing this architecture with Krtolica's system would have been implementing a known technique to improve Krtolica's known firewall traversal method to yield the predictable result of improving firewall traversal between different networks. *Id.* Finally, according to Petitioner, Krtolica recognizes that its system may be used in "an international or global internet providing electronic communication between networks and organization computer facilities around the world" (Ex. 1004, 4:17–20), and a person of ordinary skill would have been motivated to modify this system to incorporate DSDP's central controller, which is disclosed as coordinating communication in an "International Service Provider Network." Pet. 81–82 (citing Ex. 1002 ¶ 184); Ex. 1007, 39–40, Fig. 18. We find that these arguments provide a sufficiently detailed and persuasive rationale explaining why and how one of ordinary skill would have made the proposed combination.

In addition to the arguments considered above, we have also considered Patent Owner's arguments and evidence concerning objective indicia of obviousness, as discussed in detail in Section II.H below. For the reasons discussed, we find that Patent Owner's evidence purportedly showing long-felt need, unexpected results, and industry praise, does not outweigh Petitioner's evidence concerning the obviousness of claim 6. On the full record, Petitioner has established by a preponderance of the evidence that claim 6 would have been obvious over Krtolica, Rosenberg, and DSDP.

3. Claims 7, 8, 15 and 20

Patent Owner does not separately dispute Petitioner's basis for claims 7, 8, 15, and 20. Petitioner's arguments for these claims are summarized below.

Claim 7 is dependent on claim 6, and further recites the steps of:

> determining a peripheral controller connected to said external endpoint device;
>
> opening another external channel between said central controller and said peripheral controller;
>
> forwarding said multimedia communication data to said peripheral controller from said central controller; and
>
> distributing said multimedia communication data to said external endpoint device.

Ex. 1001, 14:55–63.

Petitioner argues that DSDP discloses determining a peripheral controller connected to the external endpoint device, opening another external channel between the central controller, and the peripheral controller, and forwarding the multimedia communication data to the peripheral controller from the central controller. Pet. 82–87 (citing Ex. 1007, 4, Fig. 15; Ex. 1002 ¶ 190). Petitioner further contends that both Krtolica and DSDP disclose distributing the multimedia communication data to the external endpoint device, pointing to its previous arguments for claim 5. Pet. 87 (citing Ex. 1007, 4; Ex. 1002 ¶ 193). Petitioner further argues that it would have been obvious to combine these aspects of DSDP and Krtolica as recited in claim 7. *Id.* at 82–87 (citing Ex. 1004, 1:45–47; Ex. 1002 ¶¶ 189, 191–193). Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, and DSDP teaches claim 7 by a preponderance of the evidence.

Claim 8 is dependent on claim 6 and further recites "distributing said multimedia communication data to said external endpoint device when said external endpoint device is connected to said central controller." Ex. 1001, 14:64–67. Petitioner argues that in DSDP, the remote (or external endpoint) receives this call, meaning that multimedia communication data is distributed to the endpoint. Pet. 88 (citing Ex. 1007, 4). Petitioner further contends that in DSDP, the DGK opens channel between each GK it is connected to, and the GK is then connected through the gateway to the endpoint phone in order to place the call. *Id.* (citing Ex. 1002 ¶ 194). Petitioner additionally argues that it would have been obvious to combine DSDP with Krtolica's system for the reasons previously discussed for claim 7. *Id.* at 89. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, and DSDP teaches claim 8 by a preponderance of the evidence.

Claim 15 depends on claim 14, and further recites that "said external controller communicates with a central communication controller to establish a communication channel with said second communication community." Ex. 1001, 161–4. Petitioner relies on its arguments for claim 6 above. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, and DSDP teaches claim 15 by a preponderance of the evidence.

Claim 20 depends on claim 17 and recites that establishing a third communication connection comprises:

> issuing a third communication request to a central communication controller;
>
> establishing a first central communication channel between said first external controller and said central communication controller;
>
> issuing a fourth communication request from said central communication controller to said second external controller; and
>
> establishing a second central communication channel between said central communication controller and said second external controller.

Ex. 1001, 17:5–17.

Petitioner argues that DSDP teaches these limitations for reasons similar to those discussed for claim 6, and that it would have been obvious to combine DSDP with Krtolica and Rosenberg for the reasons discussed above for claim 6. Pet. 90–95. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, and DSDP teaches claim 20 by a preponderance of the evidence.

G. Ground 4: Obviousness over Krtolica, Rosenberg, Eisenberg and DSDP — Claim 21

Claim 21 depends from claim 20 and further recites (1) "verifying said third communication request at said central communication controller prior to said establishing said first central communication channel" and (2) "verifying said fourth communication request prior to said establishing said second central communication channel." Ex. 1001, 17:18–18:6. For this claim, Petitioner references and relies upon the evidence and arguments presented for claims 2 and 19. Patent Owner argues that claim 21 is not obvious based on the deficiencies of Eisenberg for the step of "verifying," which we have not found to be persuasive. PO Resp. 51. Based on the full record (including evidence of objective indicia of nonobviousness), we find that Petitioner has established that the combination of Krtolica, Rosenberg, Eisenberg, and DSDP teaches claim 21 by a preponderance of the evidence.

H. Objective Indicia of Nonobviousness

Patent Owner also presents arguments and evidence of objective indicia or secondary considerations of nonobviousness. PO Resp. 51–57; PO Sur-Reply 19–22. Objective indicia of nonobviousness may include long-felt but unsolved need, failure of others, unexpected results, commercial success, copying, licensing, industry praise, and expert skepticism. *Mintz v. Dietz & Watson, Inc.*, 679 F.3d 1372, 1379 (Fed. Cir. 2012). "[O]bjective indicia 'may often be the most probative and cogent evidence of nonobviousness in the record,'" and "help turn back the clock and place the claims in the context that led to their invention." *Id*. at 1378 (quoting *Ortho–McNeil Pharm. v. Mylan Labs., Inc.*, 520 F.3d 1358, 1365 (Fed. Cir. 2008)). Evidence of objective indicia of nonobviousness "must always when present be considered en route to a determination of obviousness." *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling USA*, *Inc.*, 699 F.3d 1340, 1349 (Fed. Cir. 2012); *see also Apple Inc. v. Samsung Elecs. Co*., 839 F.3d 1034, 1048 (Fed. Cir. 2016) (en banc).

Objective indicia of nonobviousness are "only relevant to the obviousness inquiry 'if there is a nexus between the claimed invention and the [objective indicia of nonobviousness].'" *In re Affinity Labs of Tex., LLC*, 856 F.3d 883, 901 (Fed. Cir. 2017) (quoting *Ormco Corp. v. Align Tech., Inc*., 463 F.3d 1299, 1312 (Fed. Cir. 2006)). For objective indicia of nonobviousness to be accorded substantial weight, their proponent must establish a nexus between the evidence and the merits of the claimed invention. *ClassCo, Inc. v. Apple, Inc.*, 838 F.3d 1214, 1220 (Fed. Cir. 2016).

As the Federal Circuit has explained, "a patentee is entitled to a rebuttable presumption of nexus between the asserted evidence of secondary considerations and a patent claim if the patentee shows that the asserted evidence is tied to a specific product and that the product 'is the invention disclosed and claimed.'" *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)). That is, presuming nexus is appropriate "when the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Id.* (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). On the other hand, the patentee is not entitled to a presumption of nexus if the patented invention is only a component of a commercially successful machine or process. *Id.* Once "the patentee has presented a prima facie case of nexus, the burden of coming forward with evidence in rebuttal shifts to the challenger . . . to adduce evidence to show that the commercial success was due to extraneous factors other than the patented invention." *Demaco*, 851 F.2d at 1392–93.

However, "[a] finding that a presumption of nexus is inappropriate does not end the inquiry into secondary considerations." *Fox Factory*, 944 F.3d at 1373. "To the contrary, the patent owner is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the 'direct result of the unique characteristics of the claimed invention.'" *Id.* at 1373–74 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)). "Ultimately, the fact finder must weigh the secondary considerations evidence presented in the context of whether the claimed invention as a whole would have been obvious to a skilled artisan." *Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33 at 33 (PTAB Jan. 24, 2020) (precedential) (citing *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331 (Fed. Cir. 2016)).

i. Presumption of Nexus

Patent Owner argues that the challenged claims are embodied in its Secure Traversal Navigation Solution system (the "STNS system"). PO Resp. 52 (citing Ex. 2008; Ex. 2009 ¶¶ 228–234; Ex. 2028). Patent Owner refers to the Declaration of Rahul Vijh for support, with Mr. Vijh testifying that he considered "Source Code for directPacket's STNS system" and, based on his review, the STNS system embodies the inventions of claims 1–23 of the '828 patent. Ex. 2008 ¶¶ 9, 17. Mr. Vijh refers to a claim chart that purports to identify source code for each element of the claims. *Id.* ¶ 17, App. B. Patent Owner contends that when a marketed product embodies the claimed invention, objective evidence may be presumptively attributed to the patented invention. PO Resp. 52 (citing *PPC Broadband, Inc. v. Corning Optical Commc'ns RF, LLC*, 815 F.3d 734, 747 (Fed. Cir. 2016)).

Patent Owner refers to the testimony of Dr. Jeffay, who references the Declaration of Mr. Vijh and relies upon it for his opinion that the challenged claims are embodied in the STNS system. Ex. 2009 ¶ 232. Patent Owner also relies on Dr. Jeffay's review of a report by market research firm Wainhouse Research (the "Wainhouse report") (Ex. 2028), which provides the results of testing of Patent Owner's STNS system. *Id.* at ¶ 233.

Patent Owner argues that Petitioner fails to directly respond to and rebut the testimony provided by Dr. Jeffay and Mr. Vijh. PO Sur-Reply 19–21. More specifically, Patent Owner asserts that Dr. Jeffay provides unrebutted testimony regarding how the objective evidence offered is reasonably commensurate with the scope of the challenged claims. *Id*. at 21 (citing Ex. 2008 ¶ 17; Ex. 2009 ¶ 232; Ex. 1044, 207:9–212:3; *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013)).

As Petitioner argues, however, Patent Owner does not provide sufficient analysis demonstrating that the STNS system was coextensive (or nearly coextensive) with the challenged claims. *See* Pet. Reply 21–22. The main evidence of a nexus presented by Patent Owner is the Vijh Declaration, but Mr. Vijh's testimony on the issue merely consists of the statement that he examined source code for the STNS system, and "it is my opinion that directPacket's STNS system practices and embodies the inventions recited in Claims 1–23 of the '828 Patent." Ex. 2008 ¶¶ 9, 17. Mr. Vijh also states that, in support of this opinion, he "compiled a claim chart identifying, on a claim element-by-claim element basis, where in the STNS Source Code each element of Claims 1–23 of the '828 Patent is found," which is attached as Appendix B of the Declaration. *Id.* ¶ 17. Appendix B, however, only presents as support for each claim element a listing of subroutine names without additional detail, such as the source code for the subroutine or an explanation of its contents or operation. *See id*. ¶ 17, App. B.[13] Moreover, none of the source code for the STNS system was produced by Patent Owner. *See id*. Thus, Patent Owner has not provided Petitioner or the Board with sufficient information to understand the basis for Mr. Vijh's

[13] Patent Owner files a Motion to Seal, which seeks to seal portions of Appendix B of the Vijh Declaration, and, more particularly, seeks to seal the names of portions of the source code. Paper 29; Ex. 2008. We address the Motion to Seal below, but note that the discussion herein does not disclose the identification of portions of the source code that are alleged to be confidential.

opinion or to evaluate its accuracy. Accordingly, because the testimony is conclusory and not supported by evidence of record, we cannot credit Mr. Vijh's testimony concerning the alleged practice of the claims by the STNS system. 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

Patent Owner also relies on the testimony of Dr. Jeffay, who refers to the Vijh Declaration, and states that "I find the [Mr. Vijh's] analysis credible" and that "the conclusions developed are supported by the analysis presented." Ex. 2009 ¶ 232. Dr. Jeffay continues: "*[f]or these reasons*, it is my opinion" that the claims are embodied by the STNS system. *Id.* (emphasis added). We cannot afford weight to this portion of Dr. Jeffay's testimony because Dr. Jeffay does not base his opinion on his own independent evaluation of the source code and rather relies upon that the testimony of Mr. Vijh, which we find to be insufficiently supported and conclusory, as discussed above.

We also are not persuaded by Dr. Jeffay's reliance on the Wainhouse report. *See* Ex. 2009 ¶ 233. Dr. Jeffay testifies that "the [Wainhouse] [r]eport provides the results of extensive testing of the Patent Owner's STNS system which has been shown to embody the inventions of the '[828] Patent." *Id.* Patent Owner additionally refers to Dr. Jeffay's deposition testimony as support for the allegation that Mr. Vijh's opinions are corroborated by the Wainhouse report. PO Sur-Reply 19 (citing Ex. 1044, 207:9–212:3).

The Wainhouse report documents an evaluation of the STNS system, including testing, with assessment of different criteria, such as install/configure difficulty, user interface, connectivity, interoperability, feature sets, security, and costs. Ex. 2028, 1–4. Although the Wainhouse report includes testing protocols and results, it does not provide any details on the STNS system itself or its operation. *See generally id*. Similarly, as discussed above, Dr. Jeffay's testimony references the Wainhouse report, but provides no discussion or explanation of how the claim elements are embodied in the STNS system. *See* Ex. 2009 ¶¶ 232–233; Ex. 2028, 2, 4, 17, 20; Ex. 1044, 207:9–212:13. Instead, Dr. Jeffay testifies, in a conclusory manner, that "the [Wainhouse] Report confirms my opinion that the Challenged Claims are embodied by Patent Owner." Ex. 2009 ¶ 233. In view of the lack of information on the STNS system and its operation in the Wainhouse report, and Dr. Jeffay's failure to provide supporting explanations with sufficient detailed explanations, we cannot credit Dr. Jeffay's testimony on the alleged nexus, and the Wainhouse report does not serve to corroborate Mr. Vijh's opinion that the challenged claims are embodied in the STNS system.

Thus, based on the evidence of record, Patent Owner does not provide sufficient analysis demonstrating that the infringing products were coextensive (or nearly coextensive) with the challenged claims. *See* PO Resp. 52. We, therefore, find that a presumption of nexus is inappropriate. *See Lectrosonics*, Paper 33 at 33; *Fox Factory*, 944 F.3d at 1374.

ii. Long-Felt Need

Patent Owner asserts that its STNS system satisfied a long-felt but unmet need for a unified communication solution that allowed for multimedia communications to be carried out across multiple networks or network boundaries without compromising call quality or network security. PO Resp. 53–55 (citing Ex. 2009 ¶¶ 228–234). Patent Owner asserts that as the Internet matured and network links had increased capacity, the desire to conduct multimedia communication sessions across disparate, geographically distant networks grew and several technical challenges needed to be resolved. *Id*. at 53–54. Patent Owner further argues that efforts to address these issues began shortly after the H.323 and SIP protocols were developed, yet despite the significant attention devoted to the issue in academia and industry, no solution had emerged. *Id*. at 54.

Patent Owner contends that its STNS system satisfied this long-felt need because it "marked a significant advancement in the technology and addressed a critical problem, which theretofore had plagued the videoconferencing industry." PO Resp. 54–55 (citing Ex. 2009 ¶¶ 228–234). Patent Owner argues that because the STNS solution solved known issues without adversely impacting overall call quality and user experience, the claims satisfied a long-felt but unmet need. *Id*. at 54 (citing Ex. 2028, 12, 17; Ex. 2009 ¶¶ 228–234; Ex. 2008).

Establishing long-felt need "requires objective evidence that an art-recognized problem existed in the art for a long period of time without solution." *Ex parte Jellá*, Appeal No. 2008-1619, 2008 WL 5693899, at *13 (BPAI Nov. 3, 2008) (precedential). Furthermore, one must demonstrate that "widespread efforts of skilled workers having knowledge of the prior art had failed to find a solution to the problem." *In re Allen*, 324 F.2d 993, 997 (CCPA 1963).

Petitioner argues that the STNS system did not satisfy a long-felt but unmet need. Pet. Reply 25–26. Petitioner asserts that as of December 2004, numerous products were already in commercial use that allowed multimedia communication across disparate networks. *Id*. (citing Ex. 1042, ¶ 29). In support, Dr. Lavian testifies that by December 2004, H.323 and SIP were mature technologies that had been around for years. Ex. 1017 ¶ 30. Dr.

Lavian further testifies that at that time the industry understood how to communicate across disparate geographic networks using H.323 and SIP. *Id*.

We are not persuaded that Patent Owner has provided sufficient evidence to establish a long-felt need that the claimed invention satisfied. Patent Owner relies on the Wainhouse report for support that the STNS system allegedly solved long-felt needs, however, the report makes general statements about the STNS system, but it does not indicate that the STNS system solved any firewall traversal issues. Ex. 2028, 20–21. Additionally, Dr. Jeffay's testimony on long-felt need only provides general statements on the issue. Ex. 2009 ¶ 233.

Moreover, the lack of any evidence of actual sales or customer use of the STNS system cuts against Patent Owner's assertion that this system satisfied long-felt but unmet needs of customers. And, Patent Owner does not show a nexus between the alleged long-felt needs and the merits of the claimed invention; Patent Owner provides no additional evidence to demonstrate that the STNS system attributes met long-felt needs.

iii. Unexpected Results

Patent Owner asserts that there were real-world constraints at the time of the '828 patent that imposed significant obstacles for multimedia communications. PO Resp. 55. Patent Owner argues that "there existed real-world constraints at the time of the '828 Patent that imposed significant obstacles for implementing a unified communication solution that allowed for multimedia communications across multiple diverse network communities without [compromising] call quality or network security." *Id* at 55 (citing Ex. 2009 ¶¶ 228–234). Patent Owner asserts that given the daunting challenges at the time, a person of ordinary skill would not have expected that these goals could be achieved. *Id.* Further, Patent Owner asserts that the ’828 patent inventor’s ability to clear these hurdles was “seamless,” and accomplished what no person of ordinary skill in the art would have expected was possible. *Id.* (citing Ex. 2028; Ex. 2009 ¶¶ 228–234; Ex. 2008).

We agree with Petitioner’s argument that Patent Owner does not identify how the STNS system was any different than products that were on the market at the time. *See* Pet. Reply 27. To establish unexpected results, the claimed subject matter must be compared with the closest prior art. *In re Baxter Travenol Labs*., 952 F.2d 388, 392 (Fed. Cir. 1991). The evidence of record indicates that there were other products in the market that allowed firewall traversal with multimedia communications. *See* Ex. 2028, 2; Ex. 1017 ¶ 29. Patent Owner provides no evidence explaining the differences between the STNS system and other systems. *See* PO Resp. 55–56. Furthermore, the lack of any evidence of actual sales or customer use of the STNS system cuts against Patent Owner’s assertion that this system’s operation had unexpected results. And, Patent Owner fails to show a nexus between the alleged unexpected results and the merits of the claimed invention; Patent Owner provides no additional evidence to demonstrate that the STNS system attributes produced unexpected results.

iv. Significant Industry Praise

Patent Owner asserts that the STNS system received significant industry praise from industry thought leaders. PO Resp. 56–57. More specifically, Patent Owner asserts that Wainhouse, a respected analyst and thought leader in the videoconferencing industry, lauded the STNS system’s “seamless” operation, noting that “[a]fter installing STNS within the test environment, video calls between the different networks and firewalls worked *perfectly*." *Id*. at 56 (quoting Ex. 2028, 1). Patent Owner contends that this alleged industry recognition of the features of the claims that "unexpectedly overcame the significant limitations of the prior art solutions further confirms they are nonobvious." *Id*. at 56 (citing *Institut Pasteur & Universite Pierre Et Marie Curie v. Focarino*, 738 F.3d 1337, 1347 (Fed. Cir. 2013)).

Here, the only evidence presented in support of alleged significant industry praise is the Wainhouse report. *See* PO Resp. 56–57. We find this evidence to be insufficient to demonstrate significant industry praise. The limited nature of the evidence—one report from an evaluation company—does not rise to a level of demonstrating significant industry praise. Patent Owner fails to show a nexus between the alleged industry praise and the merits of the claimed invention; Patent Owner provides no additional evidence to demonstrate that the STNS system attributes had been found to be praiseworthy by the industry.

v. Conclusions on Objective Indicia of Nonobviousness

For the reasons explained above, we conclude that Patent Owner's evidence purportedly showing long-felt need, unexpected results, and significant industry praise is not sufficient to outweigh Petitioner's evidence of obviousness of the challenged claims.

III. MOTION TO SEAL

Patent Owner filed a Motion to Seal and for Entry of a Protective Order. Paper 29. Patent Owner seeks to seal portions of Exhibit 2008, and a version with the redactions has been filed. *See* Ex. 2008. Patent Owner asserts that Exhibit 2008 contains a claim chart with an identification of highly confidential source for the STNS system, and seeks to seal that identification. Paper 29, 1. The Motion is unopposed.

We have reviewed the redacted portion of the document, as well as the explanations of the confidential nature of the materials for which sealing is sought, as discussed in the Motion. We grant the Motion and the associated request to enter the Protective Order.

IV. CONCLUSION

Petitioner has demonstrated by a preponderance of the evidence that claims 1–23 are unpatentable.[14]

In summary:

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 3–5, 9–11, 13, 14, 16, 17, 22, 23	103(a)	Krtolica, Rosenberg	1, 3–5, 9–11, 13, 14, 16, 17, 22, 23	
2, 12, 18, 19	103(a)	Krtolica, Rosenberg, Eisenberg	2, 12, 18, 19	
6–8, 15, 20	103(a)	Krtolica, Rosenberg, DSDP	6–8, 15, 20	

[14] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceedings 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. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or 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).

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
21	103(a)	Krtolica, Rosenberg, Eisenberg, DSDP	21	
Overall Outcome			1–23	

V. ORDER

It is

ORDERED that Petitioner has shown by a preponderance of the evidence that claims 1–23 are unpatentable;

FURTHER ORDERED that the Motion to Seal (Paper 29) is granted;

FURTHER ORDERED that the request to enter the protective order is granted; and

FURTHER ORDERED, that because this is a final written decision of the Board under 35 U.S.C. § 318(a), any party to this proceeding seeking judicial review of our decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Roberg C. Mattson
John F. Presper
Oblon, McClelland, Maier & Neustadt, LLP
cpdocketmattson@oblon.com
cpdocketpresper@oblon.com

PATENT OWNER:

Jitendra Malik
Christopher B. Ferenc
Katten Muchin Rosenman LLP
jitty.malik@kattenlaw.com
christopher.ferenc@kattenlaw.com