

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioner

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00676
Patent 8,677,450 B2

Before CHRISTOPHER M. KAISER, JOHN A. HUDALLA, and
AARON W. MOORE, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4

I. INTRODUCTION

Cisco Systems, Inc. and Fortinet, Inc. (collectively, “Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–4, 7–10, 14, 16, 22–23, 25, and 27 (“the challenged claims”) of U.S. Patent No. 8,677,450 B2 (Ex. 1401, “the ’450 patent”). Petitioner filed a Declaration of Henry Houh, Ph.D. (Ex. 1403) with its Petition. InfoExpress, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 7,¹ “Prelim. Resp.”), along with declarations of Dr. Eric Cole (Ex. 2001) and Hugh Smith, Ph.D. (Ex. 2007). With our authorization (*see* Paper 9), Petitioner also filed a Preliminary Reply (Paper 11, “Prelim. Reply”) and Patent Owner filed a Preliminary Sur-reply (Paper 12, “Prelim. Sur-reply”) directed to Patent Owner’s attempt to antedate the asserted references.

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2023). Under 35 U.S.C. § 314(a), we may not authorize an *inter partes* review unless the information in the petition and the preliminary response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

For the reasons that follow, we institute an *inter partes* review.

¹ Paper 7 was filed with its availability restricted to “Filing Party and Board.” Patent Owner filed a public version of the Preliminary Response as Paper 8.

II. BACKGROUND

A. *Real Parties-in-Interest*

Petitioner identifies Cisco Systems, Inc. and Fortinet, Inc. as the real parties-in-interest. Pet. 1. Patent Owner identifies InfoExpress Inc. as the real party-in-interest. Paper 5, 1 (Patent Owner’s Mandatory Notices).

B. *Related Matters*

As required by 37 C.F.R. § 42.8(b)(2), the parties identify the following district court cases as related matters: *InfoExpress Inc. v. Fortinet, Inc.*, No. 4:23-cv-04389 (N.D. Cal. filed Aug. 25, 2023); and *InfoExpress Inc. v. Cisco Systems, Inc.*, No. 4:23-cv-02698 (N.D. Cal. filed May 31, 2023). *See* Pet. 1; Paper 5, 1. Patent Owner additionally identifies the following *inter partes* review proceedings as being related: IPR2024-00539, IPR2024-00540, IPR2024-00675, IPR2024-00677, and IPR2024-00679. *See* Paper 5, 1–2.

C. *The ’450 Patent*

The ’450 patent is titled “Systems and Methods of Controlling Network Access” and the disclosed invention lies “in the field of computing systems and more specifically in the field of network security.” Ex. 1401, 1:26–27.

The Background of the Invention section of Specification explains that “[s]everal approaches to controlling external access to computing networks have been developed” with the goals of “limiting access to authorized users and assuring that computing devices employed by these users do not include malicious computing code such as viruses, worms, or Trojan horses.” Ex. 1401, 1:29–34.

It explains that “[a] first level of access control is achieved by requiring authentication of a user,” which “may be accomplished by

requiring the user to enter a username and password or by reading a MAC address or other identifying information from an access device.” Ex. 1401, 1:38–42.

The Background further explains that “[r]eliance on mere user authentication includes several disadvantages,” including that “there are no provisions to assure that an access device used by the authenticated user meets network security policies,” which can be a problem because “[t]he access device may have out-of-date virus software, may have security vulnerabilities, or may be otherwise compromised.” Ex. 1401, 1:48–53. In addition, that approach requires that the access point “support one of a specific set of access protocols” and “[b]ecause many access points do not support VMPS, 802.1x, or a similar protocol, implementation of this approach on a large preexisting network, such as a corporate network, may be prohibitively expensive.” *Id.* at 1:53–59.

The Background next explains that “[a] greater level of access control may be achieved by including a gatekeeper between the secure network and the access device,” where “[t]he gatekeeper is configured to ensure that the access device conforms to a predetermined security policy.” Ex. 1401, 1:60–63. This is shown in Figure 1, labeled as prior art, which is a block diagram of a Secure Network 100 with “two instances of a Gatekeeper 110 each associated with a different instance of an Access Point 120.” *Id.* at 1:65–67. The access points are capable of supporting “virtual local area networks (VLANs),” which are “generated by associating communication ports within Access Point 120 with separate virtual networks.” *Id.* at 2:13–15. Thus, one access device may be placed on a different VLAN than another access device by assigning the communication ports of the access

point to separate VLANs, such that “[f]rom the point of view of these devices, the effect of a VLAN is equivalent to having a separate hardwired network.” *Id.* at 2:19–21.

The prior art GateKeeper controls access to the network by authenticating users who wish to access the network access device and by ensuring that the access device conforms to a predetermined security policy before granting access to the network, for example by making certain that the access device “has up-to-date virus software and encryption protocols as proscribed by the security policy.” Ex. 1401, 2:28–30.

The Background further explains that “[a] disadvantage of the use of GateKeeper 110, as practiced in the prior art, is that all communications between Access Device 160 and LAN 125 pass through GateKeeper 110.” Ex. 1401, 2:34–36. That could be problematic because “[t]he use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110.” *Id.* at 2:39–42. And, “[e]ven if a separate GateKeeper is used for each Access Point 120, there is no isolation between compliant and non-compliant Access Devices 160 which are attached to the same Access Point 120.” *Id.* at 2:46–50.

The Summary of Invention of the ’450 Patent describes systems and methods that “include a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets,” where “[r]equests from an access device for access to the less-restricted subset are first passed to the restricted subset.” Ex. 1401, 2:56–60. It explains that “[e]lements (e.g., a gatekeeper) of the restricted subset are then used to apply security policies to the access device and if security policies are satisfied, the

access device is granted access to a less-restricted subset of the protected network.” *Id.* at 2:60–64. “The passing of access requests to the restricted subset and granting of access are accomplished by configuring and reconfiguring a communication port of an access point” and “[a]fter access is granted, further communication between the access device and the protected network can include access to the less restricted subset.” *Id.* at 2:64–3:2.

The invention summary explains that “[t]ypically, the less-restricted subset of the protected network and the restricted subset of the protected network are characterized by Virtual Local Area Networks (e.g., VLANs) defined within the access point and optionally by access control lists (ACL) of a router, firewall, or switch situated between the VLAN and the protected network” and that “[d]ifferent VLANs within the same access point, or within different access points, may be configured to characterize a plurality of restricted subsets and/or a plurality of less-restricted subsets within the protected network.” Ex. 1401, 3:3–12.

“[N]etwork traffic directed at the protected network is initially passed through a restricted VLAN,” which “is typically restricted in the sense that it only allows access to elements of the protected network that are configured to communicate with an access device whose security characteristics are unknown or questionable.” Ex. 1401, 3:13–21. “[T]he restricted VLAN allows traffic to pass to a gatekeeper configured to receive requests for access to the less-restricted VLAN, and to determine if, and to what extent, access may be allowed.” *Id.* at 3:25–28. To grant access, the gatekeeper “sends commands to the access point in order to reconfigure a communication port to which the access device is connected,” where “[t]he

reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN.” *Id.* at 3:28–33. After reconfiguration, “network traffic can pass from the access device through the less-restricted VLAN to elements of both the less-restricted subset and (optionally) the restricted subset” and “need not pass through the gatekeeper.” *Id.* at 3:35–38.

Thus, explains the invention summary, “in various embodiments of the invention a gatekeeper is used to grant access to the less-restricted subset, and after access has been granted, most network traffic does not need to pass through the gatekeeper.” Ex. 1401, 3:38–41. This limits communications with the gatekeeper “both before and after reconfiguration of the communication port, and eliminate[s] a significant disadvantage associated with the use of prior art gatekeepers.” *Id.* at 3:46–50.

Challenged claims 1, 16, and 22 are independent. Claim 1 is directed to a “method for applying a security policy to network devices,” that includes (a) performing an authentication of a device connected to an access point, (b) scanning the device to collect information regarding the device, (c) applying a security policy that includes one or more requirements pertaining to the authentication and the collected information, where the application of the security policy takes place “in response to a gatekeeper,” and (d) configuring the access point in response to a result of applying the security policy.

Claim 16 concerns a “method of providing access over a communication network” that includes (a) receiving, at an access point, a request from an access device for access to a less-restricted network, (b) applying a security policy to the access device in response to the request,

where application of the security policy includes performing an audit of the access device, (c) providing information to the access device to improve compliance of the access device to the security policy, in response to the audit, (d) granting access to the less-restricted network based on satisfaction of the security policy by the updated access device, and (e) authenticating a user of the access device, wherein granting access is further based on the authentication.

Claim 22 is directed to a “method of providing access over a communication network,” including (a) receiving, at an access point, a request from an access device for access via a less-restricted network, (b) applying a security policy to the access device in response to the request, where application of the security policy includes performing an audit of the access device, (c) in response to the audit, providing information to the access device to improve compliance of the access device to the security policy, and (d) granting access to the less-restricted network based on satisfaction of the security policy by the updated access device, including configuring the access point to allow the access.

Notably, none of these claims appear to include structural or other limitations regarding the avoidance of network traffic through the GateKeeper, as described in the Summary of Invention.

D. Prior Art

Petitioner relies on the following prior art: U.S. Patent Application Publication No. 2004/0111520 A1, filed Dec. 6, 2002, published June 10, 2004 (Ex. 1405, “Krantz”); and U.S. Patent Application Publication No.

2004/0107360 A1, filed Mar. 13, 2003, published June 3, 2004 (Ex. 1406, “Herrmann”).

E. The Asserted Ground

Petitioner contends that claims 1–4, 7–10, 14, 16, 22–23, 25, and 27 are unpatentable under 35 U.S.C. § 103(a)² in view of Krantz and Herrmann. *See* Pet. 3.

III. ANALYSIS

At this stage, we consider whether Petitioner has met the “reasonable likelihood” standard for institution under 35 U.S.C. § 314(a).

A. Legal Standards

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We also recognize that prior art references must be “considered together

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103. Because the ’645 patent claims priority to an application filed before March 16, 2013 (the effective date of the relevant amendments), we assume that the pre-AIA versions of §§ 102 and 103 apply. However, our decision would be the same under the current version of the statutes.

with the knowledge of one of ordinary skill in the pertinent art.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citing *In re Samour*, 571 F.2d 559, 562 (CCPA 1978)).

B. Level of Ordinary Skill in the Art

Citing testimony from Dr. Houh, Petitioner contends that a person of ordinary skill in the art “would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and two years of relevant experience in networking and network security, and related fields.” Pet. 4. Petitioner also asserts that “[l]ack of professional experience can be remedied by additional education, and vice versa.” *Id.*

Patent Owner argues that a person of ordinary skill in the art “would have had a bachelor’s degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cybersecurity.” Prelim. Resp. 1–2. Alternatively, Patent Owner argues that a person of ordinary skill in the art would have had “a master’s degree in one of the foregoing and at least two years of experience in the aforementioned fields.” *Id.* at 2. Patent Owner does not cite any evidence supporting its assessment of the level of ordinary skill. Neither party explains why or how the outcome of this case would be affected by the adoption of any of the proffered definitions of a person of ordinary skill in the art.

For purposes of this Decision, we adopt Petitioner’s definition of the level of ordinary skill in the art. On the present record, we are satisfied that this definition of the level of skill is consistent with the teachings of the ’450 patent and the asserted prior art.

C. *Claim Interpretation*

In an *inter partes* review, we construe each claim “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b),” which includes “construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b). Accordingly, our claim construction standard is the same as that of a district court.

Petitioner argues that one of ordinary skill in the art “would find the challenged claims unpatentable under any interpretation consistent with their plain and ordinary meaning in the context of the [']450 patent,” and thus urges that we “need not expressly construe the claim terms.” Pet. 7.

Patent Owner also argues that we should apply the plain and ordinary meaning of all claim terms, but contends that Petitioner deviates from the plain and ordinary meaning of certain limitations. *See* Prelim. Resp. 6–7. Patent Owner offers its understanding of the plain and ordinary meaning of “information regarding the device,” “providing information to the access device,” and “configuring the access point.” *See id.* at 6–10.

Patent Owner asserts that the “information” limitations “should be given their plain meaning consistent with the intrinsic evidence and not conflated with user authentication.” Prelim. Resp. 8. We note that the background section of the ’450 patent explains that authentication may be based on “reading a MAC address or other identifying information *from an access device.*” Ex. 1401, 1:38–42 (emphasis added). It thus appears that authentication can be based on device information. We need not resolve that

issue now, however, because, as explained below, we conclude that the combination contemplates use of device, not user, information.

With respect to “configuring the access point,” Patent Owner cites a statement in the specification of the ’450 patent that “[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN.” Prelim. Resp. 9 (quoting Ex. 1401, 3:31–33). Based on this statement, Patent Owner argues that “reconfiguring the communication port” includes the type of change in connections between inlet and outlet ports of the access point depicted in Figures 3A and 3B of the ’450 patent. *See id.* at 9–10. Thus, Patent Owner concludes that the “plain meaning for ‘configuring the access point’ requires there to be a change to the access point itself; not a change to something else.” *Id.* at 10.

Based on the present record, we agree with Patent Owner that the recited “configuring” at least encompasses changing the association between the input port and output port of the access point. This is supported by the specification of the ’450 patent, which states: “Access Control 320 is configured to send commands to Switch Logic 317 in order to reconfigure members of Ports 305A-305G. This reconfiguration includes modifying the association of members of Ports 305A-305G with different members of VLANs 310A-310D.” Ex. 1401, 9:30–34; *see also id.* at 8:4–12 (similar disclosure with respect to “configuring and reconfiguring”).

However, on the present record, we do not agree with Patent Owner that “configuring the access point” is *limited* to changing the association between the input port and the output port of the access point. Instead, the ’450 patent makes clear that reconfiguration is “typically,” but not

necessarily, of this type. *See* Ex. 1401, 3:30–33. For this reason, we do not adopt Patent Owner’s proposed construction at this point.

We conclude that we need not expressly construe any other claim terms at this time. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Obviousness Ground Based on Krantz and Herrmann

As noted, Petitioner contends that the subject matter of the challenged claims would have been obvious in view of Krantz and Herrmann.

1. Krantz

Krantz is a U.S. patent application titled “Increasing the Level of Automation when Provisioning a Computer System to Access a Network.” Ex. 1405, code (54). Krantz “relates to configuring computer systems to appropriately communicate on a network, and more specifically, to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network.” *Id.* ¶ 2. Figure 2 of Krantz is reproduced below.

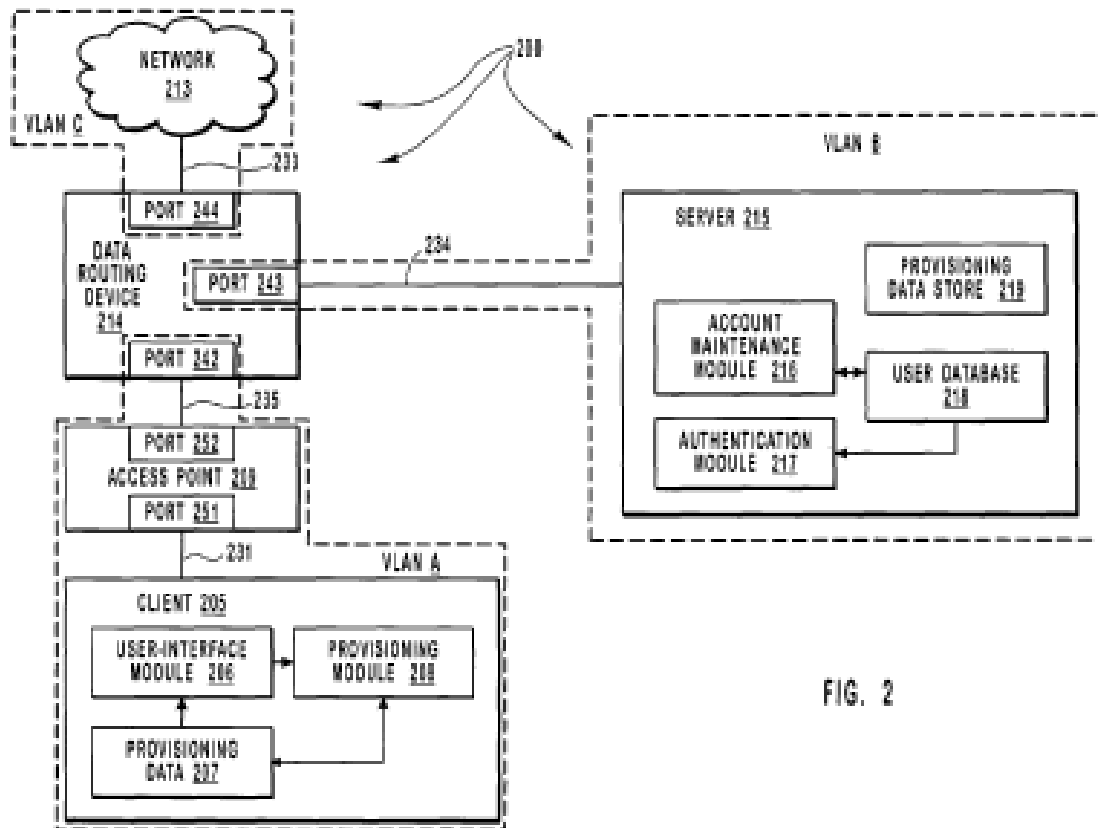


FIG. 2

Figure 2 “illustrates an example of a network architecture that can facilitate increasing the level of automation when provisioning a client.” Ex. 1405 ¶ 28.

In the system of Figure 2, “[d]ata can be transferred between access po[in]t 209 and client 205 through port 251” and “[l]ikewise, data can be transferred between access point 209 and data routing device 214 through port 252.” *Id.* ¶ 63. “Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” *Id.* ¶ 60.

2. Herrmann

Herrmann is a U.S. patent application titled “System and Methodology for Policy Enforcement.” Ex. 1406, code (54). Herrmann “relates generally to information processing and, more particularly, to

systems and methods for policy enforcement on computer systems connected to one or more networks.” *Id.* ¶ 3. According to Herrmann, “if a client device connected to a network . . . is infected with a virus or worm, it may infect other machines on the same network,” making it important to “ensur[e] that devices connected to the network are running current anti-virus programs.” *Id.* ¶ 12. To do so, Herrmann teaches a system in which a client device attempts to access a network and information is collected “from the client device” so that the system can “determin[e] whether to authenticate the client device for access to the network based, at least in part, upon the collected information.” *Id.*, code (57).

3. *Prior-Art Status of Krantz and Herrmann*

Patent Owner argues that neither reference asserted by Petitioner qualifies as prior art to the ’450 patent “because the InfoExpress inventors conceived of the invention [of the ’450 patent] before the effective dates [of Krantz and Herrmann] and exercised reasonably continuous diligence in reducing the claimed inventions to practice.” Prelim. Resp. 33–45.

Petitioner disagrees that the present record sufficiently shows that the inventors of the ’450 patent conceived of the invention before the effective date of Krantz or Herrmann and that the inventors exercised reasonably continuous diligence in reducing that invention to practice. *See* Prelim. Reply 1–7. In particular, Petitioner raises questions with respect to the independence of Patent Owner’s evidence from the inventor testimony that evidence is intended to corroborate, as well as with respect to whether the evidence offered by Patent Owner sufficiently shows conception, reduction to practice, and reasonably continuous diligence. *Id.*

We do not think the information of record is sufficient to antedate Krantz and Herrmann such that we should deny institution of *inter partes* review on that basis. First, Patent Owner’s arguments rely on the testimony of inventor Stacey C. Lum, who has not yet been subject to cross-examination. *See* Prelim. Resp. 35–45 (citing Ex. 2003). Second, Petitioner identifies several issues where further development of the record may be helpful. For example, Patent Owner’s asserted date of conception is associated with the date of an engineering specification included in the record as Exhibit 2011. *See* Prelim. Resp. 35–36 (citing Ex. 2003 ¶ 12; Ex. 2011; Ex. 2012). We agree with Petitioner (*see* Prelim. Reply 4–5) that it is unclear, based on the present record, whether Exhibit 2011 corroborates the testimony supporting Patent Owner’s conception date given that the present record does not establish the author of Exhibit 2011. *See* Ex. 2003 ¶ 22 (inventor Stacey C. Lum testifying only that “InfoExpress personnel drafted EX2011”). These and other issues relating to the prior-art status of Krantz and Herrmann are, in our view, best left for trial after full development of the record.³

4. *Patentability Analysis*

We have reviewed Petitioner’s mapping of the claims to the combination of Krantz and Herrmann (*see* Pet 19–99) and find that, on the record as it now stands, Petitioner has established a reasonable likelihood that it will prevail with respect to at least one claim. As described above,

³ Given that these claims appear to not include structural or other limitations regarding the avoidance of network traffic through the GateKeeper, as described in the invention summary, the parties may wish to consider whether the subject matter was conceived *earlier* than the date of Exhibit 2011, for example in connection with the prior art GateKeeper product.

Krantz performs authentication and Herrmann provides policy enforcement, and we have previously concluded, preliminarily, that Krantz configures an access point. *See* IPR2024-00539, Paper 13, 10–11. On this record, we agree with Petitioner that it would have been obvious to one of ordinary skill in the art to add Herrmann’s policy enforcement to a system like Krantz, in order to, for example, ensure that the network is adequately protected against viruses. *See* Pet. 14–19.

Patent Owner makes three arguments against the combination, which we address in turn.

First, Patent Owner argues that Krantz and Herrmann do not disclose the claimed “information regarding the device.” *See* Prelim. Resp. 15–21. As noted above, it appears from the ’450 patent itself that authentication may be based on device information. However, we need not decide whether that is disclosed in Krantz because Petitioner also argues that “Herrmann discloses a “policy agent (or integrity agent) 413 to retrieve information about the current security policy in operation on the client device 310.” Pet. 36. We find this sufficient to teach or suggest “scanning the device to collect information regarding the device.” We do not agree with Patent Owner’s argument that “[t]he Petition relies on Herrmann only for an agent on a device” (Prelim. Resp. 20), because the Petition specifically cites Herrmann for “retriev[ing] information about the current security policy in operation on the client device.” Pet. 36.

Second, Patent Owner argues that “Krantz also does not disclose ‘performing an audit of the access device.’” Prelim. Resp. 21. While that appears to be an accurate statement, Herrmann discloses scanning the device to collect information and applying a security policy (e.g., requiring

antivirus software) and, for the “applying a security policy” limitations, the Petition describes how it would have been obvious to one of ordinary skill in the art to have “Krantz’s server 215 (“gatekeeper”) . . . check anti-virus software like Herrmann’s policy server.” *See, e.g.*, Pet. 39–40. We conclude that the Petition sufficiently alleges that this subject matter is supplied by Herrmann.

Finally, Patent Owner argues that the combination fails to disclose configuring the access point. *See* Prelim. Resp. 27–33. We do not agree.

In “Mapping #2,” Petitioner argues that Krantz’s disclosure of the configuration of access point 209 “as a VLAN aware device [that] can insert Tag Headers into data frames received from client 205 . . . that are to be transferred to VLAN B and/or VLAN C” is a disclosure of configuring the access point. *See* Pet. 49 (quoting Ex. 1405 ¶ 64). In particular, Petitioner argues that “configuration” occurs when Krantz’s access point switches from inserting Tag Headers that enable access only to VLAN B to inserting Tag Headers that enable access to VLAN C. *Id.* This is because, according to Petitioner, port 251 does the actual insertion of Tag Headers within access point 209. *See id.* at 50 (citing Ex. 1403 ¶¶ 127–128; Ex. 1405 ¶ 107).

On the present record, we find Petitioner’s contentions regarding the “configuring the access point” limitation sufficient for institution. We find that Petitioner has made a sufficient showing of how Krantz teaches or suggests a change within the range of possible meanings of “configuration” by shifting from inserting Tag Headers that enable access to VLAN B to inserting Tag Headers that enable access to VLAN C. Dr. Houh’s testimony supports Petitioner’s argument that the insertion of Tag Headers is accomplished by access point 209. *See* Ex. 1403 ¶ 127 (citing Ex. 1405

¶ 107). This testimony appears to be uncontroverted by other evidence of record.⁴

IV. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has demonstrated a reasonable likelihood that it will prevail with respect to at least one of the claims challenged in the Petition. Therefore, we institute an *inter partes* review on the asserted grounds as to all of the challenged claims.

Our factual findings, conclusions of law, and determinations at this stage of the proceeding are preliminary, and based on the evidentiary record developed thus far. This is not a final decision as to the patentability of claims for which *inter partes* review is instituted. Our final decision will be based on the record as fully developed during trial.

⁴ With respect to “Mapping #1,” the mere fact that data is sent to one destination after having been sent to another does not appear to demonstrate that there has been any change made to access point 209, rather than merely a change at one of the other stages along the way. We do not reach “Mapping #3,” because we determine that the second mapping is sufficient.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review is instituted for claims 1–4, 7–10, 14, 16, 22–23, 25, and 27 of the '450 patent on the grounds asserted in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial, which shall commence on the entry date of this decision.

IPR2024-00676
Patent 8,677,450 B2

PETITIONER:

Scott Border
WINSTON & STRAWN LLP
sborder@winston.com

Patrick McPherson
Patrick Muldoon
David Dotson
DUANE MORRIS LLP
pdmcperson@duanemorris.com
pcmuldoon@duanemorris.com
dcdotson@duanemorris.com

PATENT OWNER:

Brian Michalek
Joseph Kuo
Brian Landry
SAUL EWING LLP
brian.michalek@saul.com
joseph.kuo@saul.com
brian.landry@saul.com