

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS INC., and FORTINET INC.,
Petitioner

IPR2024-00676
U.S. Patent No. 8,677,450

**REPLY DECLARATION OF HENRY HOUH, PH.D., UNDER 37 C.F.R. §
1.68 IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW**

I, Henry Houh, Ph.D., do hereby declare as follows:

I. INTRODUCTION

1. I have been asked to provide a reply declaration at the request of Petitioners in the matter of the *Inter Partes* Review of U.S. Patent No. 8,677,450 (“the 450 Patent”) to Lum et al.

2. I am being compensated for my work in this matter at my standard hourly rate. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this proceeding. My compensation is not contingent on the outcome of this matter or the specifics of my testimony.

3. I have been asked to provide my opinions regarding whether the subject matter of claims 1-4, 7-10, 14, 16, 22-23, 25, and 27 (“the Challenged Claims”) of the 450 Patent would have been obvious to a person having ordinary skill in the art (“POSITA”) at the time of the alleged invention, in light of the prior art. It is my opinion that the Challenged Claims would have been obvious to a POSITA. In particular, I have been asked to provide my opinions regarding whether or not the claim limitations are anticipated or otherwise would have been obvious to a POSITA under the competing claim constructions as proposed by the Board and Patent Owner in this matter. For the same reasons discussed in my April 15, 2024 Declaration (“Initial Declaration”), it is my opinion that Krantz and

Herrmann render obvious the Challenged Claims under any of the proposed claim constructions.

4. In the preparation of this declaration, I have studied:

- a. the 450 Patent, Ex.1401.
- b. the prosecution history of the 450 Patent (“450 File History”), Ex.1402.
- c. all documents referenced in my Initial Declaration.
- d. U.S. Patent Pub. No. 2004/0111520 to Krantz et al., (“Krantz”), Ex.1405.
- e. d. U.S. Patent Pub. No. 2004/0107360 to Herrmann et al. (“Herrmann”), (Ex.1406).
- f. InfoExpress’s redacted Patent Owner Response dated January 29, 2025 (“Response” or “Patent Owner Response”) and all documents referenced therein that I address below.
- g. The Patent Trial and Appeal Board’s (“PTAB”) Institution Decision for the 450 Patent and related patents.

5. In forming the opinions expressed below, I have considered: the documents listed above; the relevant legal standards, including the standard for obviousness; and my own knowledge and experience based upon my work in the field of network communications and security as described below.

6. Unless otherwise noted, all **emphasis** in any quoted material has been added. Claim terms are *italicized*.

II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE

7. My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Ex.1404. A brief summary of my relevant qualifications and professional experience can be found in my Initial Declaration.

III. LEVEL OF ORDINARY SKILL IN THE ART

8. My opinions as to a person of ordinary skill in the art (“POSITA”) can be found in my Initial Declaration. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my own experience and what a POSITA would have understood or known generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the relevant field as of the priority date of the 450 Patent.

IV. RELEVANT LEGAL STANDARDS

9. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the 450 Patent, I am relying on certain basic legal principles that Cisco’s counsel has explained to me, a summary of which can be found in my Initial Declaration.

V. CLAIM CONSTRUCTION

10. As the Institution Decision noted in a related proceeding, “Petitioner argues that a [POSITA] would find the challenged claims unpatentable under any interpretation consistent with their plain and ordinary meaning in the context of the 450 patent, so we need not expressly construe the claim terms.” IPR2024-00676 Institution Decision, 11 (internal citations and quotations omitted). Similarly, “Patent Owner argues to the contrary that we should construe the phrase *reconfiguring the communication port* as to rearrange . . . **into an altered form or to configure . . . in a new way** . . . the communication port of an access point [rather than] something else.” *Id.*, 12 (emphasis added, internal citations and quotations omitted). The Board thus explained that “Patent Owner concludes that plain meaning for reconfiguring the communication port of an access point’ requires there to be **a change to the communication port of an access point**; not a change to something else.” *Id.* (emphasis added, internal citations and quotations omitted).

11. Ultimately, the Board determined “that the recited *reconfiguring the communication port* at least encompasses **changing the association between the input port and output port** of the access point.” *Id.* (citing Ex.1401, 8:4-12, 9:30-34) (emphasis added, internal citations and quotations omitted). The Board also explained that it is not limited to that construction, however. *Id.* I also note

that Dr. Cole states that “configuration of access points could be done by changing the instructions that correspond to a particular tag header.” EX2565, ¶81.

VI. KRANTZ AND HERRMANN RENDERS OBVIOUS THE CHALLENGED CLAIMS UNDER ANY PROPOSED CLAIM CONSTRUCTION FOR “CONFIGURING THE ACCESS POINT”

12. In my Initial Declaration, I demonstrated how Krantz in combination with Herrmann discloses the “*configuring the access point*.” Ex.1403, ¶¶122-139. Krantz discloses the claimed “*configuring*” under any reasonable construction, including the constructions advanced by InfoExpress.

13. I explained in ¶123 that Krantz discloses that “access point 209 (i.e., “*access point*”) is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213). Ex.1405, [0064]. I further explained that Krantz discloses re-configuring the access point after application of a security policy. Ex.1403, ¶¶125-139.

14. I explained that Krantz demonstrates that “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.” Ex.1403, ¶126 (citing Ex.1405, [0064]; *see also* Ex.1405, [0061]). Therefore, I demonstrated that Krantz is explaining that when configured as a “VLAN aware device,” Krantz’s “*access point*” is

Ex.1428

Cisco Systems, Inc./Fortinet, Inc. / Page 6

IPR2024-00676

“*configuring the access point*” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client **that may now access VLAN C**, i.e., the “less-restricted subset.” See Ex.1403, ¶¶127-128. The “*access point*” is thus “*configur[ed]*” (and reconfigured) because it has changed its association from VLAN B to VLAN C. I also referred to four contemporaneous documents to demonstrate how the access point (and port 251) is reconfigured based on the client device becoming authorized to access VLAN C. Ex.1403, ¶¶145-147.

15. For the reasons I discussed in my Initial Declaration, the above satisfies the “*configuring the access point*” limitation under its plain and ordinary meaning. Moreover, the above demonstrates how there is a **change in the instructions provided to the access point** so that data is transferred to VLAN C instead of, e.g., VLAN B. In particular, as I explained in my Initial Declaration, Krantz discloses:

When client 205 is authorized to access resources located on VLAN C, access point **209 may enable any protocols that are currently blocked for port 251** and may insert Tag Headers” indicating that data from client 205 is to be transferred to VLAN C [the “*less-restricted subset*”]. **Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers.**

Ex.1428

Cisco Systems, Inc./Fortinet, Inc. / Page 7

IPR2024-00676

Ex.1403, ¶128 (citing Ex.1405, [0107] (emphasis added)). Krantz is therefore explaining that Server 215 is “**send[ing] commands**” to change the access point’s port instructions, which InfoExpress concedes discloses “configuration of access points.” EX2565, ¶81.

16. Krantz’s disclosure is consistent with the disclosure of the Challenged Patent: “In response, Access Control 320 sends appropriate commands to Switch Logic 317. These **commands cause changes in Port 305A**, such that communication from Access Device 230 **is no longer blocked** by ACL 340C and can now be received by elements of Less-restricted Subset 310.” Ex.1401, 9:52-57.

17. Dr. Cole admits that Krantz’s server 215 (“*gatekeeper*”) makes the determination about whether data is from an authorized user. EX2565, ¶79. He also admits that the “access point may insert a different Tag Header into the data frame to label it as corresponding to VLAN C [*“the less-restricted subset”*].” EX2565, ¶79. What Dr. Cole omits from this analysis is that Krantz’s server 215 sends commands to Krantz’s access point when client 205 becomes authorized to access resources on VLAN C, *see* Ex.1005, [0107]—*i.e.*, changes the access point’s instructions so that it operates differently—to “cause access point 209 to insert appropriate Tag Headers.” Ex.1005, [0107]. Krantz thus expressly teaches “changing how access points operate,” EX2565, ¶82, contrary to Dr.

Cole's opinion. He also conceded that client devices could not insert VLAN Tag Headers at the time based on Tanenbaum, (EX2566, Ex.1427):

Q. Well, let's go to page 334. It says -- 10 I am reading the second paragraph: (Reading) So if the originator does not generate the VLAN fields, who does? **The answer is that the first VLAN-aware bridge or switch to touch a frame adds them** and the last one down the road removes them. See that?

A. I do.

Q. [] This is explaining that a VLAN-aware device may generate VLAN fields, correct?

A. Sorry. Let me just get the context. So -- so this is in the context of sort of the older Ethernet cards. So if you're looking at Paragraph 334, as new Ethernet cards come out on the market, the hope is that they will be 802.1Q compliant and correctly fill in the VLAN fields. So this -- so the originator doesn't generate. It's talking about the older Ethernet cards, but it's saying with the newer cards that are VLAN-aware, the client would sort of fill in that VLAN tag.

Q. Okay. But so -- but you're agreeing with me that a VLAN-aware device can generate a VLAN field, correct?

A. Correct.

Ex.1422, 31:9-32:15; *see also* EX2566, Ex.1427, 334. The only way that Krantz's access point 209 would know to change the VLAN tags for given data is if it were subsequently instructed or commanded to do so by Server 215—which is what

Krantz teaches. Specifically, Krantz at [0107] (above) expressly teaches changing how input port 251 on access point 209 operates by enabling protocols that were blocked. Dr. Cole admits that reconfiguration of a port includes providing instructions to change the operation of a communication port. Ex.1422, 35:12-16 (“Q.[] it's your opinion that you can reconfigure a communication port simply by changing the configuration rules associated with that port. Do I have that right? A. Right.”). This is precisely what Krantz teaches.

18. Accordingly, Krantz's teaching, at a minimum, encompasses **changing the operation** of the access point, and is entirely consistent with the Challenged Patent's claimed “*configuring the access point*” after satisfaction of a security policy. Moreover, there is **a change to the access point** because, as I described in my Initial Declaration, access point 209 may enable protocols currently blocked for Port 251, meaning Port 251 may have been previously configured to only transfer data to VLAN B and the port was reconfigured (via commands from Server 215) to transfer data to VLAN C by shifting to inserting new VLAN tag headers into incoming data. *See* Ex.1403, ¶¶127-128. This means there was a change to the communication port of the access point itself. Indeed, as discussed previously the changed ability to route data to VLAN C demonstrates that the communication port is in an altered form and/or configured in a new way, particularly where specific software protocols are changed/newly enabled. *See id.*

Ex.1428

Cisco Systems, Inc./Fortinet, Inc. / Page 10

IPR2024-00676

19. As I also explained in my Initial Declaration, to the extent one may assert that Krantz does not disclose “*configuring the access point*”—i.e., Access Point 209 (and Port 251)—it would have been obvious to do so based on Krantz itself by combining the functionality of the Data Routing Device and Access Point of Krantz in the same device. See Ex.1403, ¶131. I further explained how the combined device would “*configure*” as necessary the communication port of the Access Point for transfer of data from a client that satisfies a security policy from VLAN B to VLAN C. Ex.1403, ¶¶132-134. I had also noted that Krantz explained that:

Data routing device 414 logically represents a computer system ... when data routing device 414 receives data from network 411, data routing device 414 can determine if the data is to be transferred to network 412 or network 413. As such, data routing device 414 **can be configured** to allow access to one network (e.g., network 412) while at the same time restricting access to another network (e.g., network 413).

Ex.1403, ¶¶133; Ex.1405, [0051]. Moreover, such a “determin[ation]” would be “**based on configuration rules,**” and “[i]t may also be that a data frame is **transferred in and out of data routing device 214 at the same port.**” Ex.1405, [0059]. Krantz’s description at [0051] shows how the data routing device can

change its configuration at its input port on the access point (i.e., “*configur[ing]*”) based on whether a client device is permitted access to one network over another. This is essentially the same as the description associated with the logical associations related to shifting the transfer of data in Figures 3A and 3B and port 305A in the Challenged Patent.

20. For the reasons I discussed in my Initial Declaration, the above satisfies the *configuring the access point* limitation under its plain and ordinary meaning because based on **configuration rules**, the access point is reconfigured to transfer to VLAN C instead of, e.g., VLAN B. *See* Ex.1403, ¶138 (citing Ex.1405, [0059] and [0060] (“Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.”); Ex.1405, [0064] (“Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.”).

21. Moreover, there is **a change to the access point** because, as I described in my Initial Declaration, **configuration rules** may determine that a data frame is transferred from a first port to a second port or alternatively, it may be determined that a data frame is transferred in and out of data routing device 214 at the same port based on what a client is permitted to access. *See* Ex.1403, ¶¶131-

Ex.1428

Cisco Systems, Inc./Fortinet, Inc. / Page 12

IPR2024-00676

139. Krantz thus describes how the data routing device can change its configuration (i.e., “*configure*”) depending on whether a client is authorized. This means there was a change to the communication port of the access point itself in the combination. Indeed, the changed ability to route data through VLAN C demonstrates that the communication port of the access point is in an altered form and/or configured in a new way. *See id.*

22. Finally, I also explained that the combined device would be further enabled to “*configur[e] the access point*” for transfer of data from an authenticated client to VLAN C because of the VLAN tagging functionality that I described in detail with respect to my initial mapping. Ex.1403, ¶138.

VII. KRANTZ DISCLOSES AUDITING A DEVICE AND AUDIT DATA

23. InfoExpress has asserted that Krantz is only related to user authentication and not device auditing. *See* POR, 18, 24. InfoExpress is wrong for three reasons.

24. First, I understand that InfoExpress’s Expert admits that “user authentication”—including the requirement for usernames and passwords—may be part of a security policy audit. Ex.1422, 8:4-16, 9:12-10:9 (“Q. Okay. And so would you agree that in the context of the challenged patents, that user authentication may be considered part of a security policy audit? A. Yes, I

would.”). I agree with him, and this is further detailed in the Challenged Patent. Ex.1401, 6:42-56, 12:9-11.

25. Second, Krantz is **not limited** to user authentication as part of its application of a security policy audit. Krantz also discloses “configuration requirements” as part of auditing a device. For example, I explained Krantz’s disclosure is consistent with the disclosure of the 450 Patent that describes requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), (Ex.1401, 6:42-56), or to authenticate an access device, or user, of the access device. Ex.1401, 11:65-12:11; Ex.1403, ¶¶110-111, 203. “Configuration requirements” are disclosed in the Challenged Patent as part of a security audit, Ex.1401, 6:42-56, and I understand that InfoExpress’s expert agrees. Ex.1422, 8:20-9:11.

26. Third, Krantz also discloses machine or client device authentication and authorization—not only user authentication. For example, I previously explained that Krantz discloses that “computer systems can attempt to authenticate with one another.” Ex.1403, ¶¶163, 203. I relied on contemporaneous evidence (Ex.1416 and Ex.1417), as well as my own understanding as a POSITA, that showed that EAP-TLS and EAP-MSChapV2 were two types of machine or client authentication protocols. Ex.1403, ¶¶78, 94-95, 162-163, 203-205. For example,

Ex.1428

Cisco Systems, Inc./Fortinet, Inc. / Page 14

IPR2024-00676

EAP-TLS includes several different methods to authenticate a **client device** to a server. Ex.1416; Ex.1417. Similarly, EAP-MSChapV2, also discloses the exchange of operating system credentials and is further described as a way to authenticate a computer using machine certificates. Ex.1403, ¶78 (“As explained in more detail below, the use of EAP-TLS (*e.g.*, Ex.1405, [0067]-[0074], [0100]) was a **known authentication protocol that would be used to authenticate client devices**. *See also* Ex.1405, [0099] (describing EAP-MSChap V2).”). Further, the specification for EAP-TLS explicitly references a number of techniques for authenticating a device versus a user. Ex.1416, 1 (“Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others. To date however, EAP methods such as [6] have focused[sic] on authenticating a client to a server.”)

27. I understand that InfoExpress’s expert agreed that the “client” in Krantz is a computer. Ex.1422, 13:23-14:3. Thus, when Krantz explains in [0068] that “[W]hen EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C,**” Krantz is explaining that it is using EAP-TLS for machine (versus user) authentication techniques to authorize the client 205 computer. Ex.1403,

Ex.1428

¶78. Finally, I also testified that Krantz's disclosure of these protocols includes machine certificates that can be submitted as credentials independent of user authentication. EX2449, 185:17-187:15.

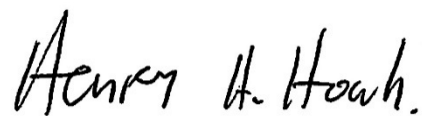
VIII. CONCLUSION

28. Thus, Krantz and Herrmann disclose these limitations under any plausible and/or articulated construction.

29. Accordingly, Krantz and Herrmann render obvious claims 1-4, 7-10, 14, 16, 22-23, 25, and 27 for this reason as well.

30. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

Date: May 15, 2025

A handwritten signature in black ink that reads "Henry H. Houh". The signature is written in a cursive, slightly slanted style.

Henry Houh, Ph.D.