PUBLIC VERSION

Trials@uspto.gov
571-272-7822

Paper # 51
Entered: August 28, 2025

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

IPR2024-00539 (Patent 8,051,460 B2)
IPR2024-00675 (Patent 7,523,484 B2)
IPR2024-00676 (Patent 8,677,450 B2)
IPR2024-00677 (Patent 8,578,444 B2)
IPR2024-00679 (Patent 7,523,484 B2)[1]

Record of Oral Hearing
Held Virtually: July 17, 2025

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

[1] This Transcript applies to each of the above-listed proceedings. Unless otherwise authorized, the parties shall not use this heading style in any subsequent papers.

IPR2024-00539 (Patent 8,051,460 B2)
IPR2024-00675 (Patent 7,523,484 B2)
IPR2024-00676 (Patent 8,677,450 B2)
IPR2024-00677 (Patent 8,578,444 B2)
IPR2024-00679 (Patent 7,523,484 B2)

APPEARANCES:

ON BEHALF OF THE PETITIONER:

SCOTT M. BORDER, ESQUIRE
Winston & Strawn LLP
1901 L Street, NW
Washington, D.C. 20036
(202) 282-5000
sborder@winston.com

ON BEHALF OF THE PATENT OWNER:

BRIAN R. MICHALEK, ESQUIRE
JOSEPH M. KUO, ESQUIRE
Saul Ewing LLP
161 North Clark Street
Suite 4200
Chicago, IL 60601
(312) 876-7100
brian.michalek@saul.com
joseph.kuo@saul.com

BRIAN LANDRY, ESQUIRE
Saul Ewing LLP
131 Dartmouth Street, Suite 501
Boston, MA 02116
(617) 912-0969
brian.landry@saul.com

IPR2024-00539 (Patent 8,051,460 B2)
IPR2024-00675 (Patent 7,523,484 B2)
IPR2024-00676 (Patent 8,677,450 B2)
IPR2024-00677 (Patent 8,578,444 B2)
IPR2024-00679 (Patent 7,523,484 B2)

ALSO PRESENT, OBSERVING :

DEVIN GARRITY
NICOLE CANDELORI
Cisco Systems, Inc.

DAKOTA KNAPP
Saul Ewing LLP

The above-entitled matter came on for hearing on July 17, 2025, commencing at 10:00 a.m., via video teleconference.

P R O C E E D I N G S

- - - - -

JUDGE HUDALLA: Okay. Good morning, everyone. We are here for the consolidated oral argument in IPR2024-00539, 675, 676, 677, and 679. I'm Judge Hudalla and joining me remotely are Judges Kaiser and Moore. So let's start with appearances first from Petitioner.

MR. BORDER: Good morning, Your Honor. This is Scott Border on behalf of Petitioner. With me is Devin Garrity and Nicole Candelori from Cisco.

JUDGE HUDALLA: Okay. Welcome to you. And from Patent Owner?

MR. MICHALEK: Your Honor, it's Brian Michalek, Counsel for InfoExpress, the Patent Owner. With me is my co-counsel, Joe Kuo, and my co-counsel, Brian Landry, and observing is one of our summer interns, Dakota Knapp (PHONETIC).

JUDGE HUDALLA: Okay, thank you. So today, we're going to have a fairly long hearing. We're going to have a first part where we're going to have a public portion of the hearing where there's a public line, so please be aware of that. And during that part, we're going to hear oral argument on Petitioner's unpatentability arguments, minus secondary considerations of non-obviousness. The second part of the hearing will be a closed portion. We'll turn off the public line and it will be on secondary considerations and Patent Owner's attempt to antedate the asserted

references.

We have two hours and 45 minutes per side of total argument. You're under no obligation to use all of that, and in fact, after we're seen the case, I'm wondering if we even need that much time. And we also have a LEAP Practitioner today, I guess, from Patent Owner. Is that still the case or no?

MR. MICHALEK: Your Honor, that's still the case. The LEAP Practitioner is going to be Mr. Brian Landry behind me --

JUDGE HUDALLA: Okay.

MR. MICHALEK: -- who will be speaking towards the antedating section.

JUDGE HUDALLA: Okay, thank you. Welcome to Mr. Landry, and so as a result, you get an extra 15 minutes of argument time, if you need it, but we'll leave that up to you. So in the first portion of this hearing today, we will have Petitioner going first and may reserve some rebuttal time, and Patent Owner will go second and may reserve some surrebuttal time.

As you know, there's a protective order in this case, so I would caution you not to reveal any confidential information in the first part of the hearing today, before we get into the closed portions. Also, I will remind all the parties to try to tell us the slide number you're on because we have all the slides in front of us, and it'll help us both now and at the time we review the transcript later on. I think that's all I have right now. So I guess, Mr. Border, are you going to be arguing first?

MR. BORDER: Yes, Your Honor.

JUDGE HUDALLA: Okay. So you can start at any time you want. I guess the question will be how long do you want to take in total and how much rebuttal time do you want to reserve?

MR. BORDER: Well, Your Honor, I was going to reserve half my time for rebuttal. I don't think I will need it and I don't think I'll need half the time to present my opening arguments either.

JUDGE HUDALLA: So you're saying you want half the two hours and 45 minutes is what you're saying?

MR. BORDER: Yes, Your Honor.

JUDGE HUDALLA: Okay, all right. You're going to make me do math here then I guess, huh?

MR. BORDER: Sorry, Your Honor. Hopefully it doesn't come into play.

MR. KAISER: Something in 30 seconds.

JUDGE HUDALLA: Yeah.

MR. BORDER: Right.

JUDGE HUDALLA: I was going to say, this is getting complicated. So 1:22 and a half. So what is that?

MR. BORDER: You know what? Let's make it an hour, Your Honor.

JUDGE HUDALLA: Okay. And --

MR. BORDER: I don't think I'll need it, but just to make things

easier for you.

JUDGE HUDALLA: Okay. And you can begin whenever you're ready, sir.

MR. BORDER: Thank you, Your Honor. Good morning, Your Honors. May it please the Court. Scott Border on behalf of Petitioner Cisco Systems and Fortinet. Before you is a series of IPRs that are relevant here. If we could go to Slide 2, please. A number of issues in dispute, this is a quick summary, all the claims at issue, but as you'll see in my presentation, I'm just going to focus on the disputed issues.

Slide 3, please. Quick roadmap of what we're going to discuss. Obviously, we're going to only go through the disputed patentability issues on this first presentation, and with that, let's go to Slide 4, please. Brief introduction of the challenged patent. On the right is Figure 2 from the patent and it's the same across all four patents that are at issue and the five proceedings that are at issue. I've highlighted the figure or the passage at left to sort of correspond with our annotated figure on the right. It's comprised of an access device, an access point, two different separated networks there, a restricted subset and a less restricted subset, and there in gray is a gatekeeper.

Slide 5, please. Again, this is just referring to the same passage. This is in the patent at Column 2, lines 52 to 65. One of the key aspects that we're going to be discussing today is the application of security policy and this notion of reconfiguring a communication port. And very briefly, the

patent uses this term "less restricted" and "restricted subset." That refers to the level of access that the access device gets when it reaches a network. It's a little counterintuitive. The restricted subset is easily accessible, but there's fewer things that the access device can do when it reaches that restricted subset. The less restricted subset is the opposite. It's harder to reach, but once you're there, there's more things that you can access.

If we could go to Slide 6, please. Again, we'll get into these disputed issues here shortly. I've broken up some of the features of the challenged patents into two issues that we'll be discussing, a security policy and this notion of reconfiguring. On the left, we have a passage from a patent -- and we're focusing on the '460 patent. They're not exactly the same across the patents, but in order to sort of streamline this presentation, I'm focusing on that.

JUDGE HUDALLA: Mr. Border, can I interrupt just for a second? I'm hearing from our folks doing the web version of this that they can't hear you. Maybe you accidentally hit the mic there. Is it showing a green light?

MR. BORDER: It is now, Your Honor.

JUDGE HUDALLA: Okay, thank you. Sorry to interrupt.

MR. BORDER: And I apologize for that. On the left here, we've got a couple different examples of the patents -- the challenged patent's description of the security policy. At the top left, this is discussing the gatekeeper, which is one of the sort of key aspects of this technology. It applies to this security policy and it gives some examples. For example, it

explains that a security policy may include requirements for user identification, such as usernames and passwords. It can include requirements, including configuration requirements relating to the configuration of the device seeking to access the protected network.

And in addition, requirements related to applications running on that access device. We've also included this passage from Column 12, lines 5 through 6, where it explains that the authenticate user step in some embodiments may be considered part of the security policy audit.

Now, to the right, I have a passage from the patent that discusses reconfiguring. This is a passage which we'll discuss in a little bit more detail later, but in sum, this is explaining how the access control of the system sends commands to the port, so that certain communications from the access device are no longer blocked. And in this sense, it's reconfiguring what the access device can access.

Can we go to Slide 8, please? Very quickly, this is -- I've highlighted in the '460 patent two of the disputed limitations I'm going to discuss. The remainder of the patents have similar limitations. In my Slides 7 through 21, we've included all of these. There's no need to go over those. Now I'm sure Your Honors are well aware of what the issues are in dispute.

Slide 23, please. Slide 23 is a brief overview of Krantz. Krantz is our primary reference and you see at right is Figure 1 from Krantz, and Krantz is Exhibit 1005. This is annotated and we've annotated in a way in order to highlight some of the features that are similar to that of the

challenged patents. So you've got an access device there at the bottom highlighted in blue, you've got an access point highlighted in green, you've got the gatekeeper highlighted in gray, and then we've got these two networks, which we've labeled -- annotated -- a restricted subset and a less restricted subset. And on the left is just a sort of corresponding description. It discusses how these are broken up, including through the use of something called a VLAN, which is also disclosed in the challenged patent.

Can you go to Slide 24, please? And again, as I did with the challenged patent, we've broken this up into sort of two categories that we're going to discuss here in detail shortly, related to a security policy and this notion of reconfiguring. On the left, we've included a passage from Krantz. This is at paragraph 16. There are a number of disclosures where it discusses this, but essentially what Krantz does is based on credentials, it determines whether or not to authorize a client for partial access to the second network or full access, as we'll discuss later.

Krantz also discusses this notion of having configuration requirements. In Krantz, those configuration requirements can be types of encryption, they can be a type of authentication, where you see EAP there. We'll discuss a couple different types of EAP that Krantz discloses shortly. One that's highlighted here is the EAP-TLS. We've got some expert testimony on what that means, and essentially, what EAP-TLS -- it's an authentication technique for clients and it's a an authentication technique for users.

And on the right, we've got a key passage from Krantz that we relied on for the reconfiguring element and it discusses how the system reacts to a client being authorized. And just as in the challenged patent -- and again, this is paragraph 107 from Krantz -- it explains that this server 215, which is the gatekeeper, sends commands to the access point to enable protocols and so that the access point can assert appropriate tag headers, and the appropriate tag headers there as doing some work, which we will discuss very soon.

Slide 25, please. Not much to say here, Your Honors, other than just to show that from an architectural standpoint, the disclosures in Krantz are strikingly similar to the disclosures in the challenged patent. Slide 26, please. This is Herrmann. Herrmann is our secondary reference. We used Herrmann for its teachings. Teachings related to ensuring that a client device has an up-to-date version of the applicable security policy. We'll discuss it briefly, but part of this insurance is ensuring that the client device has updated antivirus software. We used Herrmann for its teaching of this notion, of an application running on a client device and ensuring that it's up to date.

Slide 28, please. In our combination, which we show on the screen -- this is Slide 28 -- with evidentiary support from our expert, Dr. Houh, we showed that it would be obvious to combine Herrmann's techniques, not its physical structure, but its techniques, related to determining whether an access device is authorized for network access, and I probably should have

highlighted, including checking its antivirus software, with the authentication and authorization system of Krantz.

So what we combined was Herrmann's techniques, its teachings that one additional thing your security policy could do is just check the client device for antivirus software, making sure that it's up to date. And in our papers, and we've included our cites to our papers here, we've demonstrated not only that Krantz and Herrmann are the analogous art, we identified a number of motivations to combine.

If we fast forward to Slide 32, I just want to briefly touch on some of the arguments that you'll hear from Patent Owner. This is from the Patent Owner response at 33 to 34. Their position was that Krantz and Herrmann would not work together. Your Honors, that's a physical combinability argument. That's not sound legally. I confirmed it with their expert, Dr. Cole. I asked whether he's stating that the hardware components of Herrmann wouldn't work with Krantz. He said, no, it's the software that won't work. And I asked, so you're stating that you would not be able to physically combine them. Yes. And that's an issue, Your Honor, because it misapplies the law.

If you can go to Slide 33, please. The *Allied Erecting & Dismantling Company* Federal Circuit case is one of the seminal cases on this and it explains that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. And Your Honors, I submit that that is exactly what

Patent Owner's argument is here, that because Herrmann may be programmed in a different language, that they would be incompatible. That's not what we've argued. We've simply argued that we're applying the teachings of Herrmann to the system of Krantz.

If we could go to Slide 34, please. Back to the roadmap. I'm now going to address each of these disputed issues, beginning with this notion of configuring and reconfiguring. If we can go to Slide 36, I believe this is some of the claim language that is at issue. Oops, I fast forwarded. So in Slide 36 -- or excuse me, 37 -- I'm sorry. I'm back here. Here we are.

In the petition, we explained that Krantz discloses the claim reconfiguring because the system was initially configured to transmit data only between the client and the VLAN B or the restricted subset. And if you can back up to Slide 36, I think we showed this. So the initial configuration of Krantz is that communications from the access device must go to this restricted subset and this server 215, which we've identified as the gatekeeper.

If you can go back to Slide 37, please. After the client becomes authorized, instructions are transmitted to the access point by Krantz's gatekeeper to change the configuration of port 251, which is sitting on access point 209, so that it will insert appropriate tag headers to send the data to network 213 or VLAN C, and that's what we've depicted there on the right.

Can you go to the next slide, please? This is Slide 38 and what this

shows is a comparison between paragraph 107 in Krantz and the patent at line 9, or column 9, line 47 to 52. This is the section that we relied on. We just saw this earlier. Krantz discusses that when a client is authorized, there's a number of things that take place because access 209 may have been previously blocking communications to VLAN C.

So what server 215, the gatekeeper in Krantz, does is it sends commands, causes changes in the access point and the associated communication port so that it inserts appropriate tag headers. And what does it mean by appropriate? What it means is -- if you can go back to Slide 37. So the appropriate tag headers means that instead of having a tag header that goes to VLAN B, the restricted subset, now the communications have a tag header that sends it to VLAN C, the less restricted subset.

Slide 39, please. And this was not just Petitioner's argument, but we relied on the testimony from our expert, Dr. Houh. And Dr. Houh and Petitioner relied on four different pieces of contemporaneous evidence that talk about how VLAN aware devices work and how they can be configured and reconfigured to insert tag headers in the system that's described in Krantz, and so that once a client becomes authorized, you can change a tag header from VLAN B to VLAN C, which we've identified as the less restricted subset.

Can you go to Slide 40, please? Now in response, the Patent Owner argues that there is no evidence of any change to the access point, which instead merely performs according to its initial configuration. As I

just discussed, that's simply not true. The initial configuration in Krantz is to send data to the VLAN B, the restricted subset. After it gets the commands from the server, then it sends data to VLAN B. Under Patent Owner's own assertion, there's certainly a change in the access point and it certainly does not perform to its initial configuration.

Can we skip forward to Slide 43, please? In fact, we noted in our reply that Dr. Cole admitted that configuration of a port includes providing instructions to change the operation of a communication port. Again, that's precisely what Krantz is describing in its paragraph 107. He also stated that in his declaration, that reconfiguration of the communication ports themselves can be done by changing the instructions that correspond to a particular tag header. And then I confirmed during his deposition that this was his point, and I also asked whether you could reconfigure a communication port without physically altering the port itself. He says, that's what it says.

Slide 44. Although mapping to is sufficient to find that Krantz discloses the claim's reconfiguration, Petitioners also presented a third theory. We identified as mapping number 3. Specifically, Petitioners explain that it would've been obvious to combine the functionality of the data routing device and access point of Krantz in the same device.

And one of the reasons we explain that -- and if you can go to Slide 45 -- excuse me -- Slide 46. One of the reasons we explain that is because Krantz itself contemplates combining that functionality into the

same device. There we've highlighted in green in Figure 4 this combined data routing device. And if we go back to 45, in response, Patent Owner didn't address any of these arguments. They simply said, look back at our arguments for mapping number 2. The insertion of tag headers is not reconfiguring the communication ports, but that's not what mapping 3 is about. Mapping 3 is different. It's about this combined functionality.

And if we can go to Slide 46. And we explain this in our reply is that a POSITA would've found it obvious that the technique discussed with the respect to the data routing 214 could simply be implemented at the access point itself. And why that matters -- if you can go to Slide 47 -- is because Krantz expressly describes how that routing device, 414, can be configured to allow access to one network while restricting access to another network. And so we explained in our petition, supported by Dr. Houh's testimony, that this is also a description of configuring and then reconfiguring, based on the level of access approved.

Let's go to Slide 48, please. I'm going to turn briefly to this second disputed issue. Slide 50. And Patent Owner makes an argument that Krantz doesn't disclose this notion of protected network and this notion of a less restricted and restricted network. They accuse the Petitioners of box drawing, but as we pointed out in our papers, the challenged patents -- and this is column 6, lines 55 to 57, plainly describe that these networks can be divided logically. And below, we've highlighted some other language where it describes how it can be broken up into VLANs. Krantz describes exactly

the same thing. And I asked their expert to confirm that it could be logically divided, and he says, that's exactly what the patent says.

Slide 51, please. Again, this is just -- these are just passages from Krantz where it talks about dividing these networks into virtual LANs. Again, similar passage as in the challenged patent. Let's go to Slide 52, please. Back to our roadmap. I'm going to talk security policy. And if we could go to Slide 55.

So in the petition, we explained that the '460 patent -- and we talked about this a little bit earlier -- it has a number of examples of what may be included in a security policy. Those include user identifications, such as username and passwords. Those include configuration requirements, and it also can include requirements for applications running on the client device. We explained in our petition that Krantz discloses at least one of these and that's configuration settings, which can include supported types of encryption and supported types of authentication, including this authentication type called EAP. And on the right is some additional disclosures. Krantz describes the configuration settings in a number of places, including paragraphs 66 and 67.

If we could go to Slide 56, please. The petition also explained or showed how Krantz discloses two different authentication techniques used to authenticate not only users, but actually the device that the user is on. So it's not just authentication limited to a user, but also the device itself, as we explained in our petition. This is from pages 37 to 39. The use of EAP-

TLS, which is one of the authentication techniques disclosed in Krantz was a known authentication protocol that could be used to authenticate client devices. We also relied on paragraph 99 in Krantz, which explains that part of these configuration requirements can include whether or not operating system credentials could be used for authentication. We've included the parallel cites to Krantz at 68 and 99, there on the right, and we're going to explain very briefly why that matters.

If you can go to Slide 57, please. Our expert explained that the use of EAP-TLS and the use of EAP-MSCHAP V2. These were well known techniques used for both client authentication, device authentication, and user authentication. And we pointed out this in our petition. And Exhibits 1016 and 1017 are two contemporaneous documents that Dr. Houh relied on that demonstrate, as he suggests, that it was a well-known thing, that you could use machine credentials to authenticate a device versus just authenticating a user. So we relied on this to demonstrate that Krantz not only shows user authentication, but also device authentication.

Can we go to Slide 59, please? To the extent there's any debate whether the challenged patents' security policy can include these kinds of things that I just discussed, I asked Dr. Cole each of these questions. I asked, in the context of the challenged patents, a security policy may include requirements for username and password. He said yes. I asked him, in the context of the challenged patents, a user authentication may be considered part of a security policy audit, do you agree? Yes, I would agree with that.

I asked him, a security policy may include requirements, requirements related to the configuration of an access device. He said, yes, I would agree that would include configuration requirements. So there really is no debate here between Petitioner's position as to what may be included within a security policy and at least Dr. Cole, Patent Owner's expert.

Now, Your Honors, if you can go to Slide 60. The remaining issues -- disputed issue relate to dependent claims. I'm happy to discuss those, but those positions are well briefed in our papers. And if there are no further questions, that concludes my presentation on patentability.

JUDGE HUDALLA: Okay, thank you.

MR. BORDER: Thank you, Your Honor.

JUDGE HUDALLA: I have you using 27 minutes there.

MR. BORDER: Wow.

JUDGE HUDALLA: Excuse me. What am I saying? Twenty-four minutes. And we'll now turn to Patent Owner. So Mr. Kuo, how long would you like to take and how much would you like to reserve for surrebuttal?

MR. KUO: Let's say 30 for the presentation and 10 for surrebuttal.

JUDGE HUDALLA: Okay, and you may begin whenever you're ready.

MR. KUO: Thank you. Oh, what happened? We all saw that, right? It was up there.

JUDGE HUDALLA: It was up there, yeah. I believe we had

trouble with this maybe this past week in the same room here. Why don't we go off the record for a moment here?

(OFF THE RECORD)

JUDGE HUDALLA: Okay. We'll go back on the record here with Mr. Kuo. You may begin.

MR. KUO: Good morning, Your Honor. Joe Kuo on behalf of InfoExpress. So we'll just flip through some of these slides really quickly. We have the title page at Slide 1. We grouped the various claim limitations because obviously, there are a lot of patents here and a lot of different claims, and so to make things a little bit easier and give you a little bit of a roadmap looking back at it, we've grouped the claim limitations that are at issue.

Some of the claim limitations relate to auditing and applying a security policy to the access device. Now, we've grouped these together, but there are nuances between these two limitations, and we'll talk about that a little later, but this lays out which claims have the applying a security policy to this access device and which one shave auditing as a requirement.

As Counsel mentioned during his presentation, many of the claims have to do with configuring and reconfiguring of the -- again, it's claimed differently in the different patents. In some cases, it's reconfiguring of the communication port. In other claims, it's reconfiguring of the access point. In others, it's of the communication device. And again, those nuances do become important as we go along.

What's titled here as less restricted subset claim limitations, this is a notion of the protected network where it's separated to the less restricted subset and the restricted subset, and where the gatekeeper is located on those particular parts of the network.

Monitoring claim limitations. These are found in one independent claim, as well as some of the dependent claims in this matter. And the updating claim limitations, which again is similar to, but not exactly the same as the monitoring limitations. Monitoring, as it states, is to kind of look and see what's happening. Updating is to actually respond to that monitoring, so it's an additional feature.

JUDGE HUDALLA: Mr. Kuo, if you could just mention the slide numbers as you're going on, if you wouldn't mind.

MR. KUO: My apologies. I can go back real quick.

JUDGE HUDALLA: No, that's fine.

MR. KUO: Okay.

JUDGE HUDALLA: You can keep going.

MR. KUO: Okay, okay. And then Slide 8, this is the summary of the operating system claim limitations. These are some -- this is a limitation that's found in some of the dependent claims where the audit data is specifically described as being operating system information.

So then I will go into the obviousness arguments. Slide 9 is just the title page to that. Slide 10 is title page to the protected network having a restricted subset and a less restricted subset. As I mentioned before, when

we grouped the claims with the less restricted subsets, we're talking about the overall concept of a protected network having these two different subsets.

And this limitation is found in all of the challenged claims of the '484 patent, as well as the '460 patent. And I've provided at Slide 11 some of the claim language. It's excerpted, of course, but it shows the specific language regarding the less restricted subset of the protected network, as well as the restricted subset. And it states that the restricted subset of the protected network includes the gatekeeper, and that was referring to Claim 1 of the '484 for purposes of that statement.

And this idea of the protected network is discussed throughout the patent, but it is in -- as an example on Slide 12, we show from the summary of the invention that the protected network is physically or logically divided into a restricted subset and one or more less restricted subsets. And as you see in Figure 2 and this is from Exhibit 1501, as well as any of the 01s in the various IPRs, Figure 2 shows a rectangle around what is marked as protected network 200, and within the protected network are the less restricted and the restricted network, and I'll fast forward a little bit. And on Figure 13, it's additional discussion about the different subsets.

And then Slide 14 is from the detailed description of the preferred embodiment. Again, further description of the subsets and how they interact. So on Slide 15, I've colorized the different subsets and the restricted subset, which is indicated as 205 is shown in blue. And as you can

see, the gatekeeper 225 is located on the subset. And in purple is the less restrictive subset. So the restricted subset, someone who is trying to access, will first go to the restricted subset, be vetted by the gatekeeper, and then if they're qualified, then they were allowed to go to the less restricted subset. Those terms can be a little bit confusing, but that's the way it laid out.

And here, there's a description of what the protected network is and it says, a protected network includes a corporate network, a -- I'm sorry, we're on Slide 16. The protected network can take a variety of forms, corporate networks, telephone networks, private networks, local area networks, et cetera, and one common theme through this is that it's basically a network under the control of someone, maybe a particular entity. You see here, we have a corporate network, telephone network, private network. Those all indicate that the protected network is somebody who is -- they have a set computer architecture that they are fencing off from just unauthorized access. And so as far as the claim construction for what is the protected network and what are subsets, we're just advocating the plain and ordinary meaning.

JUDGE HUDALLA: Could I ask you about this one, Mr. Kuo?

MR. KUO: Oh, sure.

JUDGE HUDALLA: On Slide 17, you have a definition of protected network. This isn't in your briefs at all, is it?

MR. KUO: No, that's what I'm saying. It's just a plain and ordinary meaning. I don't think there's any dispute about what a network is

or what the word protected means, so I -- it's not something that we disputed or we're arguing about. I'm just putting up what I think is plain and ordinary meaning. I could come up with different ways of saying the same thing.

JUDGE HUDALLA: Right. So it seems like the issue here is really the dashed lines argument that you're making --

MR. KUO: Correct.

JUDGE HUDALLA: -- so yeah, I mean, if you want to move ahead to that, that's fine.

MR. KUO: I'm --

JUDGE HUDALLA: Okay.

MR. KUO: -- very happy to.

JUDGE HUDALLA: Yeah. Okay.

MR. KUO: So I'm on Slide 18 right now. And so Petitioner's argument, what they did was they took Figure 4 from Krantz, and they said they realize that Krantz doesn't actually mention a protected network or subsets of the network, so they created it. And so they drew dashed lines around different parts and then added the label protected network and then relabeled network 413 to be the less restricted subset and relabeled network 412 to be the restricted subset with regard to Figure 4.

And then with regard to Figure 2, they did the same thing, but they labeled the less restricted network from network 213 and server 215. They labeled that as the restricted subset, but Krantz doesn't actually talk about anything about subsets, doesn't say anything about a protected network.

That includes network 413 and network 412. Instead, throughout Krantz, it speaks to those being separate networks. And in fact, if you think about what Krantz --

JUDGE HUDALLA: Sir, doesn't the patent tell us that we can do logical networks?

MR. KUO: Sure. Logical networks isn't so much physical-physical. It's more about -- even if it's a logical network, someone is in control of that logical network, where what Krantz teaches is really about -- you think back to the early 2000s and you get a mailer like every week or almost every day from AOL saying, this is how you can access the internet. And so what Krantz was saying is we have a problem. That's difficult to do if you're on the road and you're at a hotel and airport and you want to access the internet. So rather than have to load up your software or whatever, I can get something to my service that will download the appropriate ISP software, which will allow me to then access the internet. But the internet is not part of the protected network of the -- whoever is serving that function.

JUDGE HUDALLA: Well, I guess my worry here is that you're putting a spin on the term "protected network" here and I'm not sure that's reflected in your briefs.

MR. KUO: Respectfully, I would disagree that I'm changing anything. The argument has been made throughout. We talked specifically within the briefing about how the concept of accessing the internet is not -- when through some sort of server, is not a protected element.

JUDGE HUDALLA: So basically, anything that goes out on the internet can't be a protected network in your estimation?

MR. KUO: What I've said is that the protected network is something that is controlled by some entity, whatever it might be, that this is their property that they are protected, whereas --

JUDGE HUDALLA: See, that's where I'm getting back to. It seems like you're putting that spin, like there has to be a control aspect and I'm not sure that's reflected and we don't have a claim construction or anything that tells us that.

MR. KUO: I think it's inheriting the words of a protected network, where we talk about the internet, which is just open to everybody is not a protected network, whereas the control over the -- that is in our briefing.

JUDGE HUDALLA: Okay, I understand.

MR. KUO: Yeah. And if I could refer now to Slide 20, and this is similar to Slide 19, except for it compares -- now we have a comparison of Krantz unaltered versus how Petitioner presented it. In Slide 21, Krantz discloses that server 215 is actually a radius server. And so again, this goes to what Krantz is really all about. Krantz is really all about just, I'm on the road, in the airport, and I want to get on the internet, how do I do that. So I get onto the service, I download the software that configures my computer to be able to access it according it to that ISP, and I pay my credit card, and they check to see whether my credit card goes through. And once that happens, I can access it. It's really nothing more than that.

This is the discussion from Krantz that's talking about the network architecture. And even here where it talks about -- and Petitioners rely on this portion of the specification from Krantz, where it talks about network 213 can be virtually any type of network, such as, for example, a corporate or enterprise network or the internet, we don't disagree. I mean, it says what it says. But the point here is that network 213 is never stated as being part of server 215 and therefore, being part of that same network.

So if I could go to -- this is Slide 23 -- reconfiguring and configuring limitations. And this just lays out the different claims that have that limitation. But before going to -- I'd just like to make a logical point with respect to the reconfiguring. Of course, when the network is set up and your access device is -- the access points are -- everything is put together, they have to be configured. It's still a step that is done and that's just inherent within setting up with the network. The reconfiguring or the configuring in response to an audit or to application security policy, that's all done afterwards. It's to change what had already been set up.

And Figure -- I'm sorry -- Slide 24 is simply some of the claim language and as you can see here, in the '484 patent, we have reconfiguring of the communication device in Claim 1, and then in Claims 28, 41, and 56, we have reconfiguring of the communication ports. We have -- also in Claim 57, we have configuring the communication ports. In the '460, also the communication port. In '645, we have configuring of the access point, as well as in the '444 patent and '450 patent. And so again, we're not doing

-- we're not so much doing a claim construction. I'm just saying, what is the plain and ordinary meaning of configuring just to set something up? And then reconfiguring, basic English is to rearrange what had already been set up.

Now, a key part of all this is, all the claims are very specific as to what is being configured or reconfigured. And it's a communication device -- it's the communication port is an access point, and all of those are hardware. It's all configuring or reconfiguring of hardware, and this is evident from the specification. I'm sorry, that was Slide 27 about what the claims recite.

In Slide 28, configuring and reconfiguring is discussed from the Summary of Invention. It talks of access requests being received by a communication port of an access point. So, according to the specification here, an access point is one thing and a communication port is part of the access point.

Also, from the Summary Invention, on Slide 29, it talks about configuring of traffic, sending commands to the access point to reconfigure an active communication port to which the access device is connected.

Slide 30 is similar discussion in the detailed description.

And so, let's explore what patent actually teaches that means. So, what's shown on Slide 31 is Figure 3A and Figure 3B, and it discusses access point 215. And within access point 215 are a series of communication ports which are labeled 305A through 305G. And originally

on Slide 32 -- I've zoomed in on the particular portion here. It shows, for example, that Port 305A, that the traffic is going to go to Port 305F. Now, after the reconfiguring, and this is Slide 33, port 305A, the traffic from there no longer goes to Port 305F, it goes to Port 305D. So, this is an explanation of at the least reconfiguring of the communication ports themselves within the access point.

Slide 34 is just further discussion about the reconfiguring and configuring.

So, let's look at what Petitioner's reconfiguration argument is, and it's all about tag headers. And so then, the question is -- and this is particularly from the '484 Petition, I apologize for not including it in the citation, but this is Slide 35. And also, I have an error, it's actually pages 47 to 48 from the petition.

Again, this is all about tag headers, and it says nothing about changing the ports themselves. And counsel made some mention of physically changing -- that it doesn't need to be physically changed, and the deposition testimony of Dr. Cole, with respect to that, the communication ports aren't physically changed in the sense that we don't plug one in here and plug one in over there. That's what he meant, it doesn't have to be physically changed, but there still has to be a change in the programming, or the instructions for that port and for that access point. And then -- so, he's correct. It doesn't have to be physically changed where I actually move wires, but it has to be changed in the way that it operates.

JUDGE HUDALLA: Their theory is based on virtual LANs, isn't it?

MR. KUO: It is. It is.

JUDGE HUDALLA: And so why doesn't it work for a virtual LAN?

MR. KUO: It can work for a virtual LAN, but Krantz doesn't teach reconfiguring of the ports themselves. What Krantz teaches -- and I appreciate the segue, actually.

JUDGE HUDALLA: I'm helping you out a lot --

MR. KUO: In Slide 36, what is a tag header? And this is from -- again, I apologize, this is from the Tannenbaum reference. I'll get you that citation. Now, this is Slide 36. A tag header is basically part of a data frame. It's data that's associated with an access device. It's like a mailing label; it tells you where to send things. It's not hardware. And this is explained by Dr. Cole in his declaration, it's paragraph 77 of Exhibit 2565, and this is Slide 37. I won't read it, but Your Honors will have it. And Dr. Cole goes through great detail explaining why tag headers and inserting of tag headers is not reconfiguring of hardware. Again, Slides 38, 39, and 40, those are all statements from Dr. Cole, which I know Your Honors do have that.

So, let's talk about auditing an access device. In the '484 Patent, it's recited as a policy auditor configured to audit the access device that's in Claim 1, and I'm referring to Slide 42. In Claim 39, it's recited as -- and this

is a dependent claim, but it's recited as "security policy includes an audit of the access device."

In the '444 Patent, the claim -- there's a two-way method for auditing a device, that's the actual claimed method is for auditing. And one of the steps in the '444, Claim 1, it is "applying a security policy that includes at least one requirement pertaining to the audit device." I'm sorry, to the audit data. I misspoke.

And looking at Claim 22 in the '450 Patent, and this is on Slide 43, again, what we have here is "application of the security policy, including performing an audit of the access device."

So, what does auditing mean? Well, auditing -- one thing for sure it is, it's not authentication of the user. Authentication is simply, am I who I say I am? I had to authenticate coming in here, using my I.D., that I was who I say I am. And specifically discussed within the patent itself is that mere reliance on user authentication has disadvantages, and this is in the Summary of the Invention. So, instead of relying on mere authentication, they have the additional step of auditing. And auditing includes things like: operating system status, versions, updates, et cetera, antivirus software status, Windows registry information, cookies; things of that sort, so it's about the device.

Throughout Petitioner's arguments for the auditing, they rely entirely upon Krantz. And I recall during counsel's opening that he said that Krantz is a primary reference, and that they -- they relied on Herrmann

solely for teaching of anti-virus software. It doesn't tell -- so, Krantz is the reference on which they rely for auditing and audit data. And so, this is from the IPR2024-00540, paper 13, at page 13, this is Slide 46. And this is a discussion by Your Honors about what Krantz actually teaches, and we can reaffirm ourselves, but basically Krantz doesn't teach -- and we'll just focus on Slide 47 here. I'll just go to the summary paragraph: "Petitioner has not shown sufficiently that Krantz teaches the step of auditing the device in accordance with a security policy." Krantz doesn't teach auditing.

JUDGE HUDALLA: Let me ask you a question.

MR. KUO: Sure.

JUDGE HUDALLA: Were we wrong in the institution decision --

MR. KUO: No.

JUDGE HUDALLA: -- based on their arguments that Krantz has this notion of -- what is it, supporting types of authentication, supported types of encryption; checking for those sorts of things?

MR. KUO: No, you were absolutely right. So, all Krantz -- the types of the encryption and things like that are part of the -- being able to communicate -- so, it's part of the provisioning files, and this goes back to what Krantz is really all about. Again, what Krantz is really all about is can I talk to the ISP -- can I access the ISP? Do I speak the same language and things of that nature. Nothing to do with security -- it had nothing to do with security.

JUDGE HUDALLA: Didn't your expert though agree that those

were the types of things that might be considered auditing?

MR. KUO: I don't believe so. I don't believe that he's -- not in the way that it's -- not in the way that your question is framed. Auditing is still talking about device, whether it meets security policy. And so, could it be auditing in a different sense? Perhaps in the sense that it's telling you information about the device, but it's not security information about the device. When you're talking about configurations, and the like, that's just enabling the device to communicate.

JUDGE HUDALLA: Okay.

MR. KUO: And my time is running short so I'm going to go even faster than I have been.

So, referring to Slide 48, this is Petitioner's argument, Ground 1 -- 49. Ground 1, I don't think is one that's really up for debate, it doesn't pass muster. Ground 2, we discussed why Krantz, in briefing, why Krantz does not teach auditing? And to answer your question again, the Board got it absolutely right, Krantz doesn't teach auditing of devices for security policy.

And briefly, as far as the motivation to combine, the argument that Petitioner makes is that we're saying, it wouldn't be possible to combine the physical features, and that is not the argument that we've made. Exactly as Petitioner stated, we are saying that a person of ordinary skill in the art would not have been motivated to combine the techniques of Krantz and Herrmann. And this is because, in large part -- and I'm actually just going to

talk right here.

So, what Krantz is about, as we talked about, is just accessing the internet. And Herrmann talks about network access control, and Herrmann does recognize that it is beneficial to have both user authentication as well as security -- we'll call it security policy auditing. And what Herrmann also recognizes is that the way people used to do authorization was to use a radius server. And so, the radius server, that's server side. And then when it got to -- when they said, here's the problem, we need to have both device -- make sure the device is good, that the anti-virus software is good, but they didn't just add on to the radius server. They didn't just add on to that authentication module.

What they did is they -- okay, what we got to do, we got to push all this functionality of checking the device over to the access device itself. We can put all the -- let's say, access device, you figure out what you have, you report to us, and then we'll pass it through if it meets the standard. Whatever -- you tell us what it is, we'll believe you. And that's a huge problem because the access device, it can lie, and you have this problem with spoofing.

And so, Herrmann's solution to the desire to have both was to push the functionality off to the client's side and combine it with server's side. That's not the claimed invention. The claimed invention talks about the gatekeeper being part of the protected network itself, it's all server side.

JUDGE HUDALLA: Do you dispute that Krantz and Herrmann

are analogous art to the challenged patents?

MR. KUO: No, not really.

JUDGE HUDALLA: Okay. So, this is more about the combinability of those two references?

MR. KUO: Correct.

JUDGE HUDALLA: Okay.

MR. KUO: And I see I'm just about out of time. I will further state that in -- and we pointed this out in our briefing, in Herrmann itself, it actually teaches away from a server's side solution. What Herrmann incorporates, by reference, and I can bring that up actually -- Herrmann incorporates by reference the Freund Patent, which is Exhibit 2521. Freund Patent is an earlier patent, and in this patent, it talks specifically -- and this in our -- it's in our briefing, it talks specifically about the fact that they don't use a central server, and that a central server causes bottleneck problems. And I can turn you to -- it's actually in the Summary of the Invention.

And I apologize, I'm probably going to go over time by a little bit now. So, if we look to the Summary of the Invention -- I don't know if you can see that, but I can zoom in if you can't. So, in the Summary of the Invention, it says: "The present invention provides systems and methods for client-based monitoring and filtering of access, which operates in conjunction with a centralized enforcement supervisory. In accordance with the present invention, a central filter is not employed. Instead, the present invention provides client-side filter that is controlled by centralized

authority."

And earlier -- and I apologize, it's a little bit -- it's in the -- also in the Summary of the Invention, it talks about, the reason for that is it creates bottlenecks if you have it all server side. It can, but what InfoExpress did was they solved the problem of the bottleneck in a completely different way than Herrmann did. So, Herrmann actually recognizes the problem, solves it a different way. There's no reason one would have combined Herrmann with Krantz because Herrmann purportedly already solves the problem. I have more, but I know I'm overtime so I'm going to stop there.

JUDGE HUDALLA: Okay.

MR. KUO: Unless you have some questions.

JUDGE HUDALLA: No, I don't think we do. So, I have you at 32 minutes.

MR. KUO: Thank you.

JUDGE HUDALLA: You can begin whenever you're ready.

MR. BORDER: Thank you, Your Honor. Very briefly, I've asked Mr. Garrity to pull up Herrmann -- what Mr. Kuo was just reading from was not Herrmann but a patent that is identified in the background of Herrmann. Herrmann explicitly discloses that the present invention is based on a policy server. This is in paragraph 67. We identify this in our Motion to Combine. It states: "The policy server 460, which supports the methods of the present invention, ensures that all users accessing a particular system or network, comply with the specified security policy, including access rights and

cooperative anti-virus enforcement." The entire paragraph 67 is about how the server side aspects of Herrmann assist in navigating these security policies. So, it certainly does not teach away from using a server to enforce security policies.

The second point I'd like to make, and if you can go to their Patent Owner response. This is their Patent Owner response at page 14. We heard some testimony today that -- some new testimony, some new constructions related to how this reconfiguration occurs. I note in their Patent Owner response they say as before: "Patent Owner contends this limitation requires changing the ports of the access point without limiting precisely how they are changed."

It appears during Mr. Kuo's presentation, he is trying to limit precisely how they are changed. But this is in their Patent Owner's response. Again, this is their claim construction section at line 14. And with respect to this, I will note that there were a number of slides that we just saw that had no reference to the record, and Your Honor noted that as well. They include Slide 17, Slides 26, 36 to 40, and Slide 51. These are not slides that have any reference to the papers. They shouldn't be of record in this proceeding.

And I want to finish on one point, Your Honor, if we can go to Slide 39, please. Your Honor asked, didn't your expert agree that the things that Krantz describes are all part of the examples of the security policy described in the challenged patents. I think Mr. Kuo disputed that. But I asked him these questions. And it wasn't sort of amorphous question

generally about a security policy. I said, in the context of the challenged patents. And so, he agreed with me that usernames and passwords can be part of security policy. He agreed with me that user authentication can be part of a security policy. And he agreed with me that configuration requirements related to the access device may be part of a security policy.

So, Your Honor, this was not a general statement by its expert, it was a statement that fully agrees with the types of examples we identified in Krantz as disclosing the claim security policy.

If there's no further questions, Your Honor, that includes my patentability argument.

JUDGE HUDALLA: Okay, thank you.

MR. KUO: Thank you, Your Honor.

JUDGE HUDALLA: I have you at 27 in this first part of the hearing.

MR. BORDER: Thank you, Your Honor.

JUDGE HUDALLA: You can begin whenever you're ready, Mr. Kuo.

MR. KUO: So, just a couple points. Really quickly, this is the Freund reference that I -- oh, I'm sorry, this is Herrmann that I reference that's at issue here, and this is paragraph 70 from Herrmann. And it specifically states that U.S. Patent number 5,987,611, which is the Freund Patent we talked about earlier, it states that, "The disclosure of which is hereby incorporated by reference." So, it's incorporated by reference

because they said that everything that was stated within Freund is part of Herrmann. Freund specifically teaches not to use a client side filter. I'm sorry, it specifically teaches to use a client side filter and not to have it all on the server side because that creates a bottleneck.

With regard to Counsel's last point about what Dr. Cole testified about, a security policy can, in the broadest sense, can include user authentication. When you're talking about a security policy of a device, and you're talking about -- then it's not just am I who I say I am, it's do I have the necessary operating system and things of that sort? And that's it.

JUDGE HUDALLA: Okay.

MR. KUO: Unless you have some questions.

JUDGE HUDALLA: I don't think we do. Thank you.

MR. KUO: Thank you.

JUDGE HUDALLA: So, I have you at 33 minutes for the first part of the hearing here.

So, this concludes the public portion of the hearing. So, at this point, why don't we go off the record?

(Whereupon, the above-entitled matter went off the record at 11:09 a.m.)

IPR2024-00539 (Patent 8,051,460 B2)
IPR2024-00675 (Patent 7,523,484 B2)
IPR2024-00676 (Patent 8,677,450 B2)
IPR2024-00677 (Patent 8,578,444 B2)
IPR2024-00679 (Patent 7,523,484 B2)

PETITIONER:

Scott Border
WINSTON & STRAWN LLP
sborder@winston.com

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

PATENT OWNER:

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