Trials@uspto.gov
571-272-7822

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR 2018-01512
Patent 9,565,213 B2

RECORD OF ORAL HEARING
HELD: December 18, 2019

Before BRIAN J. MCNAMARA, STACEY G. WHITE, and JOHN P. PINKERTON, *Administrative Patent Judges.*

APPEARANCES:

ON BEHALF OF THE PETITIONER:

JEFFREY D. BLAKE, PARTNER
DANIEL W. MCDONALD, ATTORNEY
Merchant & Gould
191 Peachtree Street NE
Suite 3800
Atlanta, GA 30303

ON BEHALF OF THE PATENT OWNER:

JAMES HANNAH, PARTNER
JEFFREY PRICE
Kramer Levin Naftalis & Frankel, L.L.P.
990 Marsh Road
Menio Park, CA 94025

The above-entitled matter came on for hearing on Wednesday, December 18, 2019, commencing at 1:00 p.m., at the U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia.

P R O C E E D I N G S

- - - - -

USHER: Okay, please be seated.

JUDGE MCNAMARA: Okay, good afternoon, everyone. This is the oral hearing in IPR2018-01512. I'm Judge McNamara. Judges White and Pinkerton are participating remotely, so I'd remind everyone since they're participating remotely to speak into the microphones and to identify whatever demonstrative you are referring to or whatever page of the record you're referring to so that the remote judges will be able to access them. We had a prehearing conference on December 10th and we talked about some of the issues that we might want to discuss today, so I assume you're prepared for that.

Each party will have 60 minutes of total argument time and we will do this the same way we do every other hearing, and the Petitioner will proceed first to proceed with its challenges to patentability and any pending motions they may have. You can reserve up to half of your time, but not more than half of your time, for a rebuttal. Patent Owner can then argue its opposition to the Petitioner's case, present any argument it has on the pending motions. Petitioner can then use any due time it reserved to rebut the Patent Owner's opposition, and finally we'll hear from the Patent Owner who can request an opportunity to present a brief surrebuttal on the issues that were raised in the opposition. Is everybody prepared?

MR. BLAKE: Yes, Your Honor.

JUDGE MCNAMARA: Okay?

MR. HANNAH: Yes, Your Honor.

JUDGE MCNAMARA: All right. So let's begin with the Petitioner. And if you could, actually if I could get each side to please first introduce themselves so that we have that for the record as well.

MR. BLAKE: Good afternoon, Your Honor. I am Jeff Blake, Counsel on behalf of Petitioner Cisco Systems, Inc., and here with me today is Lead Counsel Dan McDonald.

JUDGE MCNAMARA: Thank you. Is there a certain amount of time you want me to -- oh, go ahead. (inaudible) my apologies. I'm getting a little confused. Okay.

MR. HANNAH: Good afternoon, Your Honors. I guess it's afternoon in Texas, so good afternoon to all. James Hannah on behalf of Centripetal, and with me is Jeff Price. And, Your Honor, I know you like the hard copies. We have a hard copy of our demonstratives if you'd like it.

JUDGE MCNAMARA: Yes, I would. Thank you very much.

MR. BLAKE: I apologize, Your Honor. I walked --

JUDGE MCNAMARA: No, it's not a problem. It's just optional. You know, sometimes it's convenient to have it.

MR. BLAKE: Yeah, I walked off without mine.

JUDGE MCNAMARA: But it's not an issue. We've got them, so.

MR. BLAKE: Okay.

JUDGE MCNAMARA: Is there some amount of time you'd like me to alert you to?

MR. BLAKE: Your Honor, I'd like to reserve 15 minutes.

JUDGE MCNAMARA: All right.

MR. BLAKE: And if you would alert me to five minutes, that would be appreciated.

JUDGE MCNAMARA: All right, so what I'll do is I'll set the clock to 40 minutes, and that'll --

MR. BLAKE: That sounds great.

JUDGE MCNAMARA: -- let you know. Yes, I think it's set to buzzer, but you'll hear it then, at 40 minutes.

MR. BLAKE: Okay, that sounds great.

JUDGE MCNAMARA: Okay, great.

MR. BLAKE: Judge Pinkerton, Judge White, are you able to hear me okay?

JUDGE PINKERTON: Yes.

MR. BLAKE: All right, thank you very much. Your Honors, we're here today to talk again about what we refer to as the 213 patent which is Exhibit 1001. This patent was at issue in a previous IPR before the Board last month on separate grounds and now it's again here this month.

JUDGE MCNAMARA: Let me ask you a quick question about that. Because there are so many IPRs, how many patents are involved? Do you know?

MR. BLAKE: Your Honor, my firm is not handling all of it. To my knowledge, and Mr. Belnap, here, is litigation counselor and I believe the answer is it's 12 or 13 patents, total --

JUDGE MCNAMARA: Okay.

MR. BLAKE: -- in the litigation.

JUDGE MCNAMARA: All right, but the Patent Owner will probably know.

MR. BLAKE: Yes. Not all of them are under IPR, just to be clear. I think it's seven or eight of which are involved in the IPR.

JUDGE MCNAMARA: Okay, great. Thanks very much.

MR. BLAKE: If we could start with Figure 1 of the 213 patent in Exhibit 1001 just to reset the stage to kind of what's going on here. We have a system for protecting certain networks as what's disclosed in the patent, and there are a number of what you refer to as packet security gateways. They're shown in Figure 1 here as 112, 114, 116, and 118, and those packet security gateways are protecting certain different networks. There are a number of iterations of this in the figures, but the important part being that the packet security gateways are provisioned with what are referred to as dynamic security policies, and those dynamic security policies come from what's referred to as a security policy management server which is shown here as Number 120, Box 120 on Figure 1.

I'll bring up what we refer to as, or what is Claim 1 here in the patent. Claim 1 is on our Demonstrative Number 1. I'll blow it up here to kind of talk a little bit about what's required in Claim 1, and this is one of two independent claims in the patent. The other independent claim is Claim 10, and I'll discuss that a little bit later, but just looking briefly at Claim 1, what you have is the first element

recites -- what we refer to as Element 1.1, recites receiving by each packet security gateway and from a security policy management server a dynamic security policy. That comprises two things.

All right, it has a rule specifying application layer packet header information, and a packet transformation function comprising, and it's important there that it says "comprising", a packet digest logging function to be performed on the packets that comprise the application layer packet header information, and I'll get back to where that comprising comes back in when I talk about Element 1.9, the routing limitation, but that'll be a little later on.

What happens in Claim 1 is you receive the dynamic security policy and then you receive packets at the packet security gateway, and the packet security gateway identifies on a packet-by-packet basis packets that comprise the application layer packet header information you're interested in. "The" as we all know is a very important word when you're in patent drafting as it refers back to something for which there's an antecedent basis, and in limitations 1.4 and 1.6, that becomes very important.

After you identify the packets that comprise the packet header information, you perform the packet transformation function on each of the one or more packets that comprise the packet -- the application layer packet header information, so you log on a packet-by-packet basis the packets that comprise the application layer packet header information, the specific application layer the packet header information, not packets that comprise any application layer packet header information, but packets that comprise the specific application layer packet header info that you're looking for. And that logging function has three steps. You're identifying a subset of information specified by the function, you generate a record based on the subset of information you identified, and you reformat that usually which so that you would send it up to some type of central server so that it could be all, you know, aggregated and analyzed.

And finally you have a limitation that you route to a monitoring device. Each of one or more packets corresponding to the application layer packet header information in response to performing the packet transformation function, and when we get to Element 1.9, we'll focus on what is the importance of saying, "It's in response to the packet transformation function".

Briefly on the issue of claim construction, most of the terms I would think at this point in time are agreed to, the terms that have been kind of discussed between the parties in the briefing. The word "packet," the parties have come to an agreement that it refers to a layer two or layer three packet, what you would refer to as a link-layer packet, a layer two, or a network layer packet at layer three. The term "monitoring device," a preliminary construction was given to it as a device that can copy or store packets.

In the institution decision, Patent Owner now seeks what is actually a broader construction, is any device that can monitor. It says that they basically would admit that it would subsume the definition that is disclosed in the specification now and that was adopted by the Board. I don't think anything ultimately turns on the construction whichever construction is there because the construction they're arguing for now is broader, and I haven't heard them to say anything turns on that construction, so I don't know that there is a dispute or a reason to change that construction.

Ultimately it comes back down to as we discussed a month ago, the one claim construction dispute would be the term, "dynamic security policy," and that term -- if you look at our Demonstrative Number 12, that term is specifically defined in the patent at Column 4, lines 58 through 63 which provide a specific definition of dynamic security policy and it's notably in the language that we all recognize a lot in patent drafting as used herein: A dynamic security policy includes, and it goes on to recite that it can be a rule that specifies criteria corresponding to one or more packets, and identifies a packet transformation function to be performed on packets corresponding to that criteria.

Now, Patent Owner would actually attempt to narrow this rule, because this rule as it's worded can cover packets -- a dynamic security

policy that is statically created, automatically created. Patent Owner wouldn't actually try to narrow it to what is disclosed, and their argument is, well, the word, "includes" is here, but it could mean something else. Well, that's true, but includes means it has to cover at least what's stated in Column 4. And includes, what is worded here, is broad enough to cover static or dynamic policies, and that's shown, if you look to our Demonstrative 13, which is a reflection of Column 14, lines 41 through 47, which provides an example of where the patent itself calls out that administrator can manually construct a dynamic security policy, and in turn, our Demonstrative 14 goes down later in Column 14 and shows where a dynamic security policy can be automatically created.

So the specification shows both ways which is completely consistent with the earlier construction of it that's shown in Column 4, lines 58 to 63 of dynamic security policy. There is no basis for trying to narrow that. It has to include at least that much which is disclosed in the specification, and Patent Owner would try to narrow it. That's the only claim construction issue we have, so with that let me turn more to the substantive argument, and a point that has been repeatedly raised which is what is the definition -- or how do we know if something's operating on a packet-by-packet basis?

This is the focus of much discussion between the parties. I'd like to frame the discussion first, and my apologies, Judge Pinkerton, Judge White that this is not in our demonstratives, but something that I thought maybe I'd throw up just to remind everyone figure 1.2 of the main prior art reference what we're referring to as "ACNS," and it's Exhibit 1008, and I'm only going to be on it for a second to show that what you see is, which is very similar to what we saw in Figure 1 of the 213 patent are what was referred to as "content engines," which we believe are the packet security gateways that

the packets flow through, and those content engines implement policies on a packet-by-packet basis that were provisioned down from what's referred to in the ACNS guide as a "content distribution manager," which it's our contention that that constitutes the claimed security policy management server.

So packet-by-packet basis, where does it come in? Well, it starts in what we've identified as Element 1.4 of Claim 1 which is shown on our Demonstrative Number 4. It is the identifying step. Identifying by the packet security gateway from amongst the packets associated with the network protected by the gateway, and on a packet-by-packet basis, you're identifying one or more packets that comprise the specific application layer packet header information that you're looking for. And in the ACNS guide, that specific application layer packet header information is what's referred to as the "HTTP Request Method," as shown on our Demonstrative 22 where ACNS on page 8-23 bleeding over to page 8-24, but I've called up page 8-23 here, talks about the fact that ACNS looks at these HTTP requests methods, and what are some examples? I'll highlight it here the way it's shown on the demonstrative.

Some examples of those request methods would be for instance, a GET request method. If I was going to put out a GET request to get certain information about a particular HTTP application. That's the specific application layer packet header information that's disclosed in ACNS and when you look at Element 1.4, again doing back to Demonstrative 4, the identifying step, you're looking for packets that comprise application layer packet information, the application layer packet information that ACNS would be looking for would be that request method.

Patent Owner's contention is because ACNS's vergerd (phonetic) in the term "request," or "responses," that you're not talking about it on a packet-by-packet basis, instead what you're talking about is reassembly, and then looking at the packets after they've all been reassembled back into an HTTP message. Respectfully ACNS never mentions reassembly and never talks about it, and the reason it doesn't is it doesn't have to operate that way. It can perform the analysis on a packet-by-packet basis. Here's how it does, though. You can think of it in one of two ways because you'll get the packets in one of two ways. First, I don't think either party contends or contests, excuse me, that all of the information for an HTTP request can fit within a single packet, a packet byte-size. As we know an application layer packet, I think Judge Pinkerton and Judge McNamara, we've talked about before.

An application layer packet to be transmitted over the Internet medium would be embedded within a TCP packet which would in turn be embedded within a network layer packet, and it's only a certain size that you can embed in any one given network layer packet and a rough approximation is 1,500 bytes. And anything you see below 1,500 bytes, if your entire request is below that, you can fit it all in one network layer packet and it can be transmitted on a packet-by-packet basis as one packet. And both sides acknowledge that.

Dr. Goodrich, Patent Owner's expert, during his deposition, which is found -- the relevant testimony is on our Demonstrative 29, he acknowledged that an application layer HTTP packet including both its headers and payload could be embedded within one layer three packet, and that's Exhibit 1026 at page 28, lines 3 through 9. So there's really no argument between experts as to whether or not you could fit everything in

one packet. Our expert, Dr. Jeffay, says in many instances, if not most, that's what you've got when you get an HTTP request or a response, and ACNS, itself, as we can see from our Demonstrative Slide 19, it itself shows examples of HTTP request that fit within one packet.

JUDGE MCNAMARA: But let me ask you this: Is that what it's about or is ACNS about reassembling it and you get the situation where it's a trivial case when it all fits in one packet?

MR. BLAKE: I don't think I would call it a trivial case, because I don't know that it's --

JUDGE MCNAMARA: Well, none of it's trivial. One thing we know from all this documentation is there is nothing trivial about this.

MR. BLAKE: And respectfully that's not what it's about.

JUDGE MCNAMARA: Mm-hmm.

MR. BLAKE: There's no discussion of ACNS, and I'm going to try to get to it quickly, talking about if you have the multiple packet scenario --

JUDGE MCNAMARA: Okay.

MR. BLAKE: -- what's going on, but I think whether you have one packet or multiple packets, given what ACNS is looking for, which is the request method, you don't need reassembly in order to identify what's going on. You can operate on a packet-by-packet basis, and the experts do recognize that in many, if not most cases, your request is going to fit within one packet, so there's no need to reassemble. Once you get to the endpoint, right, you have a stream coming into the content engine, you have a stream coming out of the content engine, it's going to be packetized in both cases, and when you get to a client, maybe, it's going to have to be reassembled.

But at the point the time you're in the content engine, the content engine to perform its work, it can be a single packet, and in of the law for it

to be obvious, the person of ordinary skill in the art to know you could do something on a packet-by-packet basis. If there's an embodiment, like single-packet embodiment that's disclosed to a person of ordinary skill in the art, that's enough. The single-packet embodiment should meet the limitation. For instance, what I've got here as Demonstrative 19 shows a log format for a pack that has 1,100 bytes. It would all fit within -- the application layer packet would fit nicely within one network layer packet. This is Exhibit 1008 at page 19-1. It shows it'll all fit nicely within one packet and you could process it without having to reassemble anything, and the system would process it without to reassemble anything.

Similarly there's a second disclosure on a separate format on the very next page, Exhibit 1008 at 19-2. We are using the native page numbers here, but that's shown in our Demonstrative Number 20, and I'll call it up. It shows another packet where you have a byte-size. Let me highlight it so we can all -- look, what we were talking about, a 632 bytes. Again it fits within one packet.

Now, Judge McNamara, to your point, some requests are not going to fit within one, and the Patent Owner has cited in an example from ACNS that shows a byte size of 3632, I believe. That doesn't fit within one. That'd be multiple packets. But ACNS doesn't need to reassemble that to identify the specific application layer packet header information that it's looking for, which would be the request method, and the reason is, that request method, and I don’t think either side contests this, would be at the beginning of the application layer packet headers, and so when you break up that application layer packet to put it in separate network layer packets, the first network layer packet is going to have the application layer request method. It's going

to have that specific application layer packet header information you're looking at.

So when it's received by the content engine of ACNS, a person of ordinary skill in the art would understand that it can identify, okay, I've got a flow of packets coming in, and in that flow of packets, the first one tells me that this is a supported request method or it's not a supported request method for an HTTP request. And I know what to do with that, and I know how long the string of packets is going to be and so I know what to do with this packet and the packets that follow it.

JUDGE MCNAMARA: But the packets that follow don't have that same identifier, right?

MR. BLAKE: That's correct.

JUDGE MCNAMARA: Okay, so the question then becomes whether or not it's packet-by-packet or because of this, that it's a group of packets and in the case where everything happens to fit into the one message, the one packet, then it's just still packet-by-packet, so I think that -- and I'm not sure I'm articulating this as eloquently as it's been described, but that's my sense as to what we're talking about.

MR. BLAKE: If we look at what the claim says you have to do in this element, and there's really two elements, right, 1.4 is the identifying step, 1.6 is the logging step. I want to get to that in a moment and kind of through the same analysis --

JUDGE MCNAMARA: Sure.

MR. BLAKE: -- but it does seem like this is a key point for everyone. It says, we're identifying on a packet by packet basis one or more packets comprising the application layer of packet header information. So you can look at each of the packets. You're looking for that application layer packet

header information; if it's there, you're going to identify it. That's all that's required by the claim. You have to identify one or more packets that comprise the application layer of packet header information in order to take the step.

Now, you may know the length of the entire application layer of packet and therefore know that the next end packets are going to correspond to the overall request.

JUDGE MCNAMARA: What's the significance of the "or more," one or more?

MR. BLAKE: I would say the significance of it is it is an acknowledgement of the fact that it could all be in one packet, and therefore you are acting on packet-by-packet. Just like ACNS acknowledges with its examples, and the experts acknowledge, it could all be in one packet and therefore, I have one packet and then I've got to have another packet right behind it, that everything could be in one packet. "Or more" acknowledges that an ACT request could fit across more than one packet and the amount of application layer of packet header information that you're looking for could be so much that it has to go into two-network layer packets, right, and in an application layer packet, you can have any number of headers, and so it could be that those headers themselves actually span more than one network layer of packet if you have more than 1,500 bytes of them.

Now in the ACNS disclosure that's not going to happen. Because what ACNS is looking for is not a 5-tuple or other types of information. It's looking for the request method, and I think that's a key part of ACNS, is that when it's looking for the request method, that's going to be in the first packet, so, you know, the application layer packet header information, the specific information you're looking for, and I think that's important, right?

Again, it says "the application layer packet header information" is what you try to identify, referencing back to the previous limitation that identified the rule.

In ACNS, that specific information is always going to be in the first packet, and you're going to be able to say, okay, I have this packet and then the packets that are still part of the flow would relate that same request that has that support method and the next time I see a packet that has a new support method, it's going to be a new request, and maybe that new one will be one packet, maybe it will be more than one packet, but I know how to handle that situation. I think that's the significance of one or more, is it's just acknowledging that your application layer packet header info could be in one packet or more. In the ACNS scenario because everyone agrees that the request method is at the beginning of the packet, it's always going to be in the first packet.

JUDGE MCNAMARA: Okay. Thanks.

MR. BLAKE: I think while we're talking a little bit about that claim language, there's another set of claims, Claims 4 and 5, that also are relevant. I think we should look at those kind of briefly. In our Slide Demonstrative 9, has Claim 4 which depends from Claim 1. So it's talking about that identification step. If you look at this about halfway, the third line of Claim 4 says, "We're in the identifying step of the one or more packets comprising the specific application layer packet header comprises determining by the packet security gateway that the one or more packets comprising the application layer header information are amongst the one or more HTTP packets," right, so what that's saying is determining that the packets that have the application layer header information are among the stream or flow

of HTTP packets, and then Claim 5 which is our Demonstrative 10 builds further on that.

So let me back out of Claim 4 and put Claim 5 up there. Because importantly what Claim 5 says is what you're talking about is that the one or more packets comprise an HTTP GET method call. So what you're looking for in Claim 5, what you're trying to identify is that one or more packets, that request method just like ACNS, the HTTP GET method call is what you're looking to identify on page -- in Exhibit 1008 of ACNS, page 8-23. It talked about the request method and it gave an example of a GET method call. Here it likewise talks about that in the patents.

The patents -- we're talking about similar, if not exact same subject matter, and what importantly Claim 5 says to your point, Judge McNamara, is it could be one packet that comprises that GET method call. The GET method call could be in more than one packet in which case you can still look for the specific application layer packet header information on a packet-by-packet basis, even where you have more than one packet that corresponds the get method call or the request as it were. That's what ACNS is doing. It doesn't have to reassemble. The patent acknowledges, basically, you don't have to reassemble to do this. ACNS doesn't have to reassemble to do this. It can look at the first packet and say, okay, I have a get method call; is that supported or not supported? If not, this is what I do. If so, this is what I do on the identification step.

Now, the second claim element where a packet-by-packet analysis is relevant is what we call Element 1.6 which is the performing step. It's the performing in the packet transformation function. And I'll throw it up on the screen here. It's in Column 15 of Exhibit 1001, and it says that, and this is important, the language and the way it is, because, again, it's talking about

the specific packet header information, performing by the security gateway and on a packet-by-packet basis, the packet transformation function on each of the -- and the one or more packets comprising -- and this "the" right here is very important -- comprising the application layer packet header information, and it goes on to say the performing of the function comprises logging steps, a digest logging, right. So what I'm doing is I'm performing the packet transformation function on each packet comprising the application layer of packet header information, the particular application packet of header information that you're looking for.

You're not logging every packet that has any application layer packet header information. That's not what the claim limitation says. It says you're performing the transformation function on the packets comprising the application layer header information. Again, you've got to look back to the antecedent basis. It's the specific information you're looking for, and I think Your Honors were asking in the prehearing conference what are some of the differences between the party. I think this point about the logging function emphasizes one of the differences between the parties on this packet-by-packet argument. If we look to the surreply put in by Patent Owner, this is Paper 22. I'll pull up page 7, and my apologize. To the judges who are on the screen, I apologize. We didn't have this in a demonstrative, but I wanted to blow this up --

JUDGE WHITE: We have the papers.

MR. BLAKE: Okay, great. Thank you. Paper 22, page 7. What Patent Owner says is it's characterizing this Claim Element 1.6, and it says that -- it refers to logging information about each packet that includes application layer packet header information, and I'll put my arrow right over here between the words, "includes and application layer of packet

information," because this sentence, it doesn't have the "the" from the claim. Excuse my poor English there, but the "the" matters in the claim because the claim says that you're performing the logging transformation function on the packets that have the specific application layer of packet header information, not as Patent Owner says in its surreply that you would log each packet that has any application layer of packet header information.

They forgot the "the" because you only log packets that have the specific application layer of packet header information that you're looking for, and that makes sense, right, the idea of what's going on in the claim is I see a packet, it's got this packet header information such as the request method that's discussed in ACNS, discussed in Claim 5. I see that particular information; I need a log entry for it for that request. I need to have a log entry for that request because either it's supported or it's not supported, the whole request. But I'll log based on the packet that has that application header information.

It tells me whether or not the request -- what the request method is. I don't need a log for every packet that's part of the request that might have application layer header information. I see the specific application layer header info that I want, and I create one log based on that. So I think the fact that the surreply is missing the "the" that comes from the claim is important in this particular situation. Again, very similar to what we talked about with Element 1.4.

When you're logging if you have a packet size such that the HTTP request fits nicely within one packet, it's the 1,100 bytes that we saw from page 19-1 of ACNS, and everything fits in one packet then you're going to log on a packet-by-packet basis, de facto. And, again, that in itself teaches a person of ordinary skill in the art that this claim limitation is obvious. But

even because what you're looking for is the supported request method, even where you have application layer header information that goes across multiple packets because the request goes across multiple packets, what you're doing is the packet that has the specific application layer of packet header information that you're looking for, that triggers the logging function.

That's what triggers the fact that you're going to have to log and when you trigger the log -- now, what can be in the log can be information about that packet. It could be information taken from the other packets that all creates one log, but the idea is that you have one log entry for one HTTP request method. That's why the system would work the way that it would and the idea that what the claim language says is you're logging the packets that have the specific application layer header information in them, so I see that specific header on a packet, the request method, create a log. Next time I see a request method, create a log. If I have multiple packets that comprise a request method, what I do is I look at it and I say, okay, in this situation the first one tells me the request method; I need to create a log. That log can contain information about the other packet from the other packets because they're all about the same request, but I create one log entry per request.

JUDGE MCNAMARA: Now, further down on that same page that you just cited, that's where the Patent Owner comes back with this argument that that's not packet by packet, right? Because the very next transaction can be split over multiple packets, and I think you said, well, the next one, you create a log. The next one you create a log, but it may not be the next packet.

MR. BLAKE: Yes.

JUDGE MCNAMARA: Okay.

MR. BLAKE: That's correct. And what would happen is if you get two packets in a row and they're both -- and everything fits within one packet both times, you're doing packet by packet. But if I get a single packet and the next one is multiple packets, you look at that first packet and you say, oh, this has the specific information you're looking for, that triggers a log.

JUDGE MCNAMARA: Okay.

MR. BLAKE: And the next time I have a packet that has the specific information I'm looking for, that triggers a log.

JUDGE MCNAMARA: That triggers a log. All right. But you maintain that that's still a packet-by-packet basis because that you've identified in the first packet the application information and then you don't need it again, right, until you get it to the next one?

MR. BLAKE: Yes, that's correct.

JUDGE MCNAMARA: Okay.

MR. BLAKE: Unless anyone has any other questions about that, I want to move on to a different limitation and a different part of the discussion which is -- and excuse me for jumping around. I'm kind of trying to cover the issues that I think are most disputed here, and we can get back to anything that's of interest to anyone here, but I'd like to talk now about Element 1.9, which is called up in our Demonstrative Number 7. It is the routing limitation. I'll call it up; I'll put it up here on the screen.

And it says routing by the packet security gateway and on a packet-by-packet basis to a monitoring device. We talked earlier about the construction issue. Each of the one or more packets corresponding to again, "the application layer packet header information, that specific information, and the issue just currently raised by the Patent Owner is, is it in response to

performing the packet transformation function? And again, we should go back to the claim language because that's the key. What is -- when you say you have to operate in response to performing the packet transformation function, the first question it begs is, what's the packet transformation function we're talking about?

And for that, we have to look back earlier in the claim to see the antecedent basis. And if I look earlier in the claim to where the packet transformation function is first identified, and this would be in our Demonstrative Number 1, has the entire claim. It says, "You have a packet transformation function comprising a packet digest logging function." So the word "comprising" has a meaning in patent law. It means that it is, not includes, but is not limited to a packet digest logging function. The packet transformation function can be broader than that. And that's obvious; we see that if we scroll further down the page and look at Claim 2 which depends from Claim 1.

And Claim 2 says, "The rules indicates performing an except packet transformation function comprising the application layer packet header information wherein performing the packet transformation function comprises forwarding." So this gives us an example of what else can be included in the packet transformation function, a forward. You can have the packet digest logging function; you can have the forward. Claim 3, I won't bring it up, but it similarly says there's something else that can be in the packet transformation function. It's a drop or a deny. But for our purposes, what's practically relevant is the forward because Element 1.9, the routing limitation, is taught in the art by the Kjendal (phonetic) reference which is Exhibit 1009.

And the Kjendal reference what it teaches, what it adds to the analysis is that you are looking at and mirroring packets based on selective information taken from the application layer packet header, and you don't mirror all packets. You mirror selective packet information, and you mirror that information off to what's referred to as a network logger. It also refers to the fact that you can mirror it off to an IDS device. Anyway it would be something that definitely constitutes a monitoring device under the Board's definition, and you mirror that information, and how do you mirror it in response to performing the packet transformation function? Well, as we just saw, the packet transformation function from Claim 2 in the 213 patent, we learned can include a forward, so what does Kjendal do?

Kjendal looks at the packets when they come in, it identifies a certain application layer packet header information. It talks about the facts specifically that can identify application layer information, and one cite I would give you is Exhibit 1009, Column 8, line 59 to Column 9, line 3. It's in our briefing, but that's one example, and it says, "Based on that, I've identified what I want. I'm going to forward it. And I will forward it off to what is the monitoring device." So in response to performing the packet transformation function, the packet transformation function is a forward in response to a determination that these selective packets should be forwarded. I make the determination to forward and then the action is it's actually routed off to a network logger or some other device.

Kjendal teaches this claim limitation. Indeed in the related proceeding to this which is IPR2018-01386, in the institution decision because Kjendal was used also for this limitation, that the Board itself looked at this limitation and found just that logic applies, and I would cite to

Paper 8 at page 31 in that related decision which of course is preliminary, but the logic still applies.

Absent any questions, I'll turn to the motivation to combine the references, and specifically the motivation to combine ACNS and Kjendal. A person of ordinary skill in the art would look at these two references. They're both -- there is no question between the parties. It's agreed that they both relate to security, system security. At least Kjendal does and there's on page 1-9 of Exhibit 1008, ACNS, even Dr. Goodrich has cited that page as noting that it teaches system security.

The argument first starts with saying well these references shouldn't be combined because Kjendal admittedly talks about packets, but Patent Owners says that ACNS talks about reassembled language. We've already talked about that. The second flavor of Patent Owner's argument that there's no motivation to combine, which also is incorrect, is to say that, well, there's no problem in ACNS that's been identified because ACNS teaches authentication, logging authentication errors, and you're using Kjendal to teach logging other types of information. Well, that, if you think about it, it makes absolute sense.

And the ACNS reference came out in 2008 -- around that's the date we're providing it, around 2008, and what it say is we're going to log certain information, but you don't want to overload a server, right, and if you look at ACNS Exhibit 1008 at pages 19-19 to 19-22, it says, "We're going to log certain information, but we don't want to log every packet," because you might overload the server. Is that my time?

JUDGE MCNAMARA: Well, that's 40 minutes, anyway, yes.

MR. BLAKE: Okay. I'll wrap it up here.

JUDGE MCNAMARA: Okay.

MR. BLAKE: We're going to overload the server. Well, what we want to do is it'll only log certain things, and typically at this point in time authentication errors is what people are concerned with, so let's log that, because that will save server space and log that. Kjendal comes along five years later and in that intervening five years, there are a number of different types of ways that there are viruses and malicious malware and software that comes up and so Kjendal teaches us you can log for other types of stuff, a whole vast array of other things because there are new types of problems we have to be worried about in security analysis, and so it teaches, look, let's log for these other types of things including application layer packet header information which may be indicative of security systems problems.

Let's make sure we look at that; let's make sure that we take what's there, log what we need to. Kjendal, itself, also acknowledges that you don't want to overload the server. You have to, you know, use specific types of information that's going to be logged, and I would cite you to Kjendal at Column 34, lines 51 to 54 where it's just like ACNS. It says we don't want to overload the server. We want to make sure that we log more information. It's more robust. It teaches you that in this new day and age as of the time of the invention of the 213 Patent, there are more things to be concerned about, more types of things that you would want to log other than just authentication errors, but you still have to be careful to analyze specific things so you don't overload the server, just as ACNS was concerned with that.

And finally in my remaining time, I'll touch briefly on the issue of the public accessibility of ACNS. There have been some arguments about it. Respectfully to Patent Owner, this is not really the type of case where you would think of an ACNS public accessibility argument in my opinion

because this is a product guide, ACNS. It's given out for a product from a big company like Cisco who is very open about saying we put everything on our website. Now, the ACNS guide, itself, says, hey, all our product documentation is on our website, Cisco.com. It says look at the audience. It's intended for a person of ordinary skill in the art. It's intended for network administrators at large sophisticated clients who are going to get it and we have every interest -- it's important to us, in fact, that we provide that information.

JUDGE MCNAMARA: But it's for those who purchased the product, not just generally available; is that right?

MR. BLAKE: It's for those who purchased the product. There is no indication of the ACNS guide where it says that documentation is on Cisco.com/tech support which is a specific location; there's no indication that that was private.

JUDGE MCNAMARA: Okay.

MR. BLAKE: That you couldn't get that. Now, the product documentation, DVDs, were also provided, but that would go to customers. But the customers are the relevant persons of ordinary skill in the art. I mean, the law supports the fact that even if it's a group of only customers, that's enough, because those are the relevant persons of skill in the art and that's what ACNS says, we're going to administrators. They're the relevant people who matter and care about using a product like this.

The release notes at Exhibit 1028 say the same thing, right. They're dated in the prior art timeframe and they refer back to the ACNS guide and say to those relevant people, if you need this information you can have it. Release notes obviously, they come about -- when you have an update to the product software you have to submit release notes to say it. That's not the

prior art relying on, but the release notes what they say is, hey, ACNS was out there. They point to say, again, all our product literature, it's on Cisco.com. We've put everything out there. It's all there. And the declarations, the two from Mr. Fuchs, which are Exhibits 1012 and 1027, he was the product manager for this product and he said unequivocally -- he said it there at his deposition testimony.

He says it there, "This product was provided -- the documentation, the ACNS, not just the product. That ACNS was provided to customers, and it was provided through the website, it was provided in product DVDs, and he cites the fact that the ACNS guide and the release notes as evidence of that, and what they say. Yes, he performed a Google Search, but that search is a red herring. That's not a real issue. All he does remind himself of what documentation proved his memory that this was provided to customers during the prior art timeframe.

JUDGE WHITE: So just to be clear, you're relying on actual dissemination not on indexing and such, but actual dissemination?

MR. BLAKE: That's correct, Judge White. We're relying on the actual dissemination through the website, through product documentation, DVDs, and that the guide and the release notes specifically say that to corroborate that point, and Mr. Fuchs' sworn testimony is corroborated by the guide and the release notes of actual dissemination. But I will make one note and then I'll sit down. The release notes point you -- if you were asking about an indexing issue, the release notes point you to the Cisco.com website and where you can find it. It says that the guide and all the documentation can be found at Cisco.com/tech support, so it does point you specifically to where you can find it on the website. Okay.

JUDGE MCNAMARA: All right. All right, you have 15mintues left.

MR. BLAKE: Thank you.

MR. HANNAH: Judge White and Judge Pinkerton, if I put something on the ELMO, can you see it? Because I remember in our last room I thought you were able to see it; can you see it here?

JUDGE WHITE: Sometimes we can. Why don't we try it out. Just throw something up there so we can just --

MR. HANNAH: Okay. We'll try that.

JUDGE WHITE: Any old thing, test it out.

MR. HANNAH: Try to -- can you see it?

JUDGE WHITE: I do not, but maybe they can --

MR. HANNAH: No magic today?

JUDGE WHITE: So they've switched the camera over, so we can see it.

MR. HANNAH: Oh, all right. Okay.

JUDGE WHITE: It's a little small, though.

MR. HANNAH: A little small. I don't know how to zoom that in. Oh --

JUDGE WHITE: But if you're just going to be relying to something in the record, I have the record in front of me.

MR. HANNAH: Okay.

JUDGE WHITE: And it's easy enough for me to just -- if you just tell me exhibit such-and-such, page whatever, that's easy enough for me to get to.

MR. HANNAH: Okay, great. I kind of like to dance around up here a little bit to keep people entertained, so I might do both just to keep it entertaining here.

JUDGE MCNAMARA: Mr. Hannah, is there a certain amount of time you'd like me to alert you to?

MR. HANNAH: Let's do the same thing, 15 minutes for rebuttal.

JUDGE MCNAMARA: So I'll give you -- I'll set it at 40.

MR. HANNAH: Perfect.

JUDGE MCNAMARA: And then you can figure out what to do after that.

SPEAKER: Do you want it in the laptop (inaudible) or do you want (inaudible)?

MR. HANNAH: No, we'll do the Elmo; you know, try that out and if it doesn't -- if I start fumbling around then I'll switch it back. All right, Your Honor.

JUDGE MCNAMARA: Ready to proceed?

MR. HANNAH: Your Honors, first off, I'd again like to say thank you. Thank you on behalf of my client. All three of you have heard this before, but it does mean a lot to my clients. They do want to thank you for your time and diving into the record, and may it please the court. The Petitioner, they lost this case with their reply. In the reply, and standing up here, they agreed that a packet is a layer two or a layer three packet that we're dealing with with regard to the 213 Patent. The ACNS reference which is relied on for numerous limitations that we'll get into simply does not involve layer two or layer three packets. It deals with HTTP, HTTP messages, HTTP transactions, not layer two and layer three.

If we look at Exhibit 1010, this is --

JUDGE MCNAMARA: Let me ask you a quick question because you just talked about the Petitioner reply and you're correct. I mean, the -- I'm sorry, your reply -- I'm sorry. The --

MR. HANNAH: Petitioner's reply?

JUDGE MCNAMARA: Never -- yes. Yes, you said that you agree that the -- it actually says you agree that packet refers to the layer two and layer three packets --

MR. HANNAH: Absolutely.

JUDGE MCNAMARA: -- and your position is that that is not what ACNS -- that's not what the reference is referring to?

MR. HANNAH: Absolutely, Your Honor.

JUDGE MCNAMARA: Okay, all right. Thanks. I would clarify that.

MR. HANNAH: Well, and let's jump to that. So what is ACNS? ACNS is a content delivery network. That's what it's about. The content engines that the Petitioner points to, those are web proxies, and those web proxies can cache content. I think Your Honors knows what a web proxy is. It acts on behalf of a web client. So a request goes to a web proxy and then on behalf of that client it'll send the request to an origin server, which is just a website. They call it an origin server. The web proxy receives that content and then will take that content and send it to the client.

Now, counsel got up and says, and I wrote it down, "For the content engine to do its work, it works on a packet-by-packet basis." That's absolutely not true. In order for a web proxy to work, it has to reassemble those messages. It has to take all of the messages for every request that comes in. It has to reassemble those because to the origin server, it has no idea where that request actually originated from. The origin server sees it because it's a proxy, sees it as coming from the proxy, and then the origin server will send a response and that goes to the proxy.

JUDGE MCNAMARA: In fact, that's part of the reason for the proxy to be there, right?

MR. HANNAH: Absolutely. That's what the proxy is for so that it can cache that response and then sends a new message, brand new response to the client, and the client has no idea. So it must reassemble. That's how it does its work. It can't do its work on a packet-by-packet basis. Now, I was going to point to -- or I will point to Exhibit 1010. Exhibit 1010 is cited by Petitioner. I'm going to try to monitor it here, and, oh, now I see a picture of myself; we don't want to see that. But if we look -- and I'm just trying to show the document (inaudible) -- oh, I see what you're doing. You're going to have to move the camera, okay. And maybe I won't do this, but anyway, Exhibit 1010. It says right here in the first lien on page 1, "The hypertext transfer protocol is an application level protocol." Application level. Everyone agrees application level is different than layer two and layer three. So every time you see HTTP and ACNS or in this record in general, that is referring to the application layer. That is not referring to layer two and layer three. And that's based on the record -- that's based on Petitioner's submission of the HTTP specification. Now, this goes to the slide deck instead. (inaudible). So if we look at the claim language and I'm looking at Slide 3 of our slide deck, just Claim 1.

There are several limitations here that are addressed and they're addressed in our briefing. There's a couple that I want to focus on here in the beginning and then I can focus on the rest later, but I want to focus particularly on the identifying limitation where you identify packets on a packet-by-packet basis, layer two/layer three packets that comprise application layer header information, and then I want to focus on the identifying -- a subset of information -- this is now on page 3 or Slide 3 of

our demonstratives -- and the generating of the record for each of those packets and it's specified by the packet digest logging function.

Now, what does the Petitioner point to for these limitations? In the Petition on page 42 for the identifying of a subset of information they cite to 19-1 and 19-5 of ACNS, and they say that on a packet-by-packet basis that this identification is happening. And if Your Honors could turn to 19-1 of the ACNS reference which is Exhibit 1008, what do they point to? They point to this squid log format example and they say that this example -- and it was highlighted in the Petitioner's opening remarks -- that this shows that ACNS is focused on packet by packet. Well, first off, I already showed you that HTTP -- anytime it talks about HTTP, we'll talk about application layer, so that's what this reference is about. It's about content. It's about content that's cacheched. But let's look at this because I think this gets a little lost in the briefing. This squid log format example cannot be a single packet. It's impossible. And I'll tell you why that this transaction log does not show this. You see it has a series of numbers and then it says, "TCP_Refresh_Miss/304". That can't be the request. That's the response; 304 is the status. That's the status of the response that comes back from the origin server. We can go to page 27 of Exhibit 1010 and it gives a whole list of status codes. 304 means that the content was not modified. TCP_Refresh, what does that mean? That means the proxy couldn't find it in its cache. So I ask you, what single packet is this showing? Is it the packet from the client to the router? Oh, it can't be that because we have a response. Is it the packet from the router to the content inspection engine? It can't be that one. We have a response, too. Is it the packet from the content inspection engine to the origin server? Oh, it can't be that. There's no replace of an IP address in here. It has the IP address of the original host

of the client that sent it, and it has a response. Okay, it's the packet that comes from --

JUDGE WHITE: Counselor --

MR. HANNAH: Yes?

JUDGE WHITE: -- if I understood he argument, though, they were not saying that every single one of these would be a single packet, but that in some of these instances, the information could fit in a single packet. So maybe this particular instance in this log file was not a single packet but others were. (audio word drop) messages that are going to take more than one packet, but some that don't.

MR. HANNAH: Your Honor, I beg to disagree. If you look at page 8 of the reply; turn to page 8 of the reply and this is, you know, I'd like to do my magic with here. This is what they say, "This is an example of a squid log entry for a single packet." That's their argument. Their argument is that this is a log entry for a single packet. Once you go back through the record and you read it, you will see that their entire argument -- if you read the paragraph before, on page 8, they say that, "ACNS teaches that the logging is performed on a packet-by-packet basis." PO acknowledges that ANCS guide discloses logging, however PO argues that the logging is performed on complete transaction and not a packet-by-packet basis. Again, PO is mistaken.

ACNS discloses sample log entries that apply to a single packet. That's their argument. And it has to be their argument because if the transaction is multiple packets, it doesn't generate a record for on a packet-by-packet. They have to make that argument. And when you look at the log entry, itself, it has to be multiple packets. And I wanted to just finish this for the record why it has to be multiple packets. It can't be just the response

packet because I covered the flow from the client to the content engine and back. It has the GET request in there, so it can't be the response packet. That's what HTTP transactions are all about. They're about the request and the response as one. That's why it's an application level protocol.

A transaction is the back and forth to see what happens in the transaction. It is completely absent any indication that it would do any type of logging on a packet-by-packet basis. And it doesn't make sense in ACNS because ACNS is about content delivery. When you look at the preference which is in the Petition they cited in 1-1 and 1-2, it's talking about content delivery and web proxies and content cacheing. You operate at the application level; you do not have to deal with anything lower than that. It doesn't make sense. When you look through the references and you look through the records, when it talks about content that's being stored and evaluated, it talks about how the webmaster is handling the content, not the network administrator. It has no notion at all of handling things on a layer 2/layer 3 packet-by-packet basis.

And, again, this is what Petitioner cited when it talks about 1-11: Content is usually stored on file servers or webservers that are not part of the ACNS network of managed devices. Content-from-content provider is often placed on the origin server by a webmaster who uses the content to build the website or multiple websites. So any indication that we're working on packets or packet level is simply not taught by ACNS. Now, this goes through several of the --

JUDGE MCNAMARA: Do you agree now, or do you completely disagree that there are circumstances where everything fits in one packet?

MR. HANNAH: I do not agree that a transaction can fit in one packet. HTTP transaction is a transaction that's coming -- okay, and let me

back up, so I want to be very clear in the context of ACNS, I want to say, that it can't be because it's a web proxy, right. The way that a web proxy works is it's going to look at the back-and-forth communication not even between it and the origin server but between the information that it gets from the clients that it's servicing. So it's looking at that entire transaction that's going back and forth, so when it talks about transactions in ACNS, it cannot fit in a single packet.

Now, there is some questions about, well, if there is certain data for a request, could that be in the single packet. That's not what we're talking about with ACNS. When they're talking about ACNS they're talking about transactions and transaction logging and that's the only thing that's cited in both the Petition and the reply. For the element of identifying a subset of information, the only thing that's cited is 19-1 through 19-5; that's these transaction logs. If I look at 19-2, there's another example of a transaction log, and what does it have? It says the transaction log is GET, and, again, I'm not using the Elmo, so if you look about halfway in the page, this was another one that was cited as an example of a log file format.

It says, "GET HTTP.www.Cisco, HTTP 1.0; the next number, 200. You know what that 200 is? That's the status. That means okay. Again turn to page 27 of 1010, 200 means okay as the status code. And just to show you, how do I know that these are the status codes? I'm going to go back to 19-1. It says specifically that it has the squid log -- and I'm flipping back to 19-1, I'm looking at the bottom half of the page, and it says, "The squid log file format is as follows: Time elapsed, remote host code/status. That status is the response code. That's the status of the HTTP application layer protocol which tells us what the status is of that request. The HTTP request

is the application layer request. So when I go and I see 200, again it shows what is the status.

So in the Petition they cite 19-1 through 19-5. That's it. That is their entire proof for the identifying element, identifying a subset of information specified by the packet digest logging function for each of the one or more packets, each of the one or more layer 2/layer 3 packets comprising application layer header information. I go to the next limitation, the generating. You have to generate for each of the one or more packets a record comprising the subset of information. In our briefing we talk about there's no packet transformation function, there's no subset. I want to make it even simpler for purposes of today. There's no generating a record at all on a packet-by-packet basis. The only thing that they cite in the Petition is 19-1.

JUDGE MCNAMARA: So let me ask you this.

MR. HANNAH: Yes?

JUDGE MCNAMARA: Let's assume that we agree with you that ACNS is not on a packet-by-packet basis, okay; is that our answer? I mean, why would the claim limitations not be obvious in view of what's disclosed in ACNS even if it's not on a packet-by-packet basis?

MR. HANNAH: All right. So, number one, that argument was never raised in the Petition, so it's not in the record, number one --

JUDGE MCNAMARA: Okay. But we focused on this term, "packet-by-packet," and it's sort of a narrow focused argument and I want to --

MR. HANNAH: Sure. And that I'm trying to make the simplest argument for -- and that's what -- you know, and I --

JUDGE MCNAMARA: Sure.

MR. HANNAH: -- you've probably known that's what I'm trying to do is to highlight, kind of the high-level arguments, but so why is it not obvious on a packet-by-packet basis?

JUDGE MCNAMARA: Right. Right.

MR. HANNAH: Because ACNS is made for a content and delivery system, made for webmasters -- that's what I just cited on 1-11 -- who post content on websites. It's not for engineers that are working on a layer 2 or layer 3 basis. There's just absolutely no notion of that at all. So you can't go in and say I'm going to log -- you know, that I'm going to handle HTTP requests, but it's obvious because I'm handling the highest layer protocol that I'm actually going to dive in and now go to layer 2/layer 3. That's the reason that they have the application layer protocol, so you don't have to do that. I mean, that's how webmasters and content providers, you know, make -- that's what they do; it's their gig, right? I mean, they go on and they make websites and you post content and you say, so some other engineer is going to be able to handle the dirty details on that communication. All I have to deal with is, you know, making a website look good. And so when you look at a content distribution network, any CDN, you're not going to be thinking layer 2/layer 3, so it's absolutely not obvious. And when you look at these transactions, oh, these are HTTP transactions. That's what it says. You know, every time when you reread the Petition and you reread the reply, every time you see HTTP, when they point to HTTP messages or HTTP, right there that's a red flag. That's application layer, and that's throughout the Petition; it's throughout the reply because they have to. That's what this is based on.

I mean, and further support for that is, the Fuchs' testimony. I don't think that it gets any clearer than -- in terms of testimony. In terms of

testimony, we've got a fact witness, not a paid expert. We got a fact witness who's the product manager, and under the heat of cross-examination, he's asked very specific questions, and I didn't take this deposition, so I'm not trying to give myself any, you know, props or anything for it, and he is very honest in it, and this is Slide 13 of our slide deck, and he was asked specifically, does -- and I'm going to ignore the security part right now.

The security part, they came back with a rebuttal that -- oh, it's the security because it's -- the word "security" in the manual. I can get into that. That's talking about authentication. That's not talking about packet security. It's in our briefing. I think that's very clear. But the part they didn't even address in the supplemental declaration is at line 16 through 19: Does it -- and it's referring to the manual, the ACNS system, does it look at individual packets within the request? It does not. That's the product manager. You can't get clearer testimony than that. And it makes sense. It's a content distribution network that operates at the highest possible layer.

So this testimony right here is dispositive to the issue. It's unrebutted. It was not addressed. When you go through the record and you look in the supplemental declaration, he doesn't touch this because he'd be lying, and he doesn't want to perjure himself for a -- I mean, he only addressed the security and he points to this, you know, line in the security saying, well, it does security, but that's because it says it in the manual even though his testimony is that, you know, to be specific, does it perform any security analysis on the request itself? It does not. I mean, that's pretty clear. He goes back and tries to fix it, but he doesn't touch the fact that deals with individual packets. That's not what ACNS does, and that's the only thing that's pointed to for these limitations.

So for the identifying limitation, and then for the generating limitation, we have -- or identifying, we have 19-1 to 19-5. That's the transaction logs that it goes through. But only for the -- the generating of the record is only 19-1. For the reformatting limitation, we have to reformat for each of the packets, each of the one or more packets, the subset of information. Again, the only thing pointed to is 19-1, and I've just shown you how it's impossible that that applies to a layer 2/layer 3 packet. It can't. It doesn't even want to. I mean, there's no reason for it to.

If there are no questions on that, I'm going to move to the routing limitation. So for the routing limitation, this is also highlighted in our briefing, and, you know, we pointed it out in our Patent Owner response. I think we made it extremely clear. We said that there's no proof that there's this routing that's done in response to performing the packet transformation function. And I guess we're -- Jindal. I guess Kjendal. I mean, pronunciation.

JUDGE MCNAMARA: KJ (inaudible).

MR. HANNAH: Yes. How are you doing it, Your Honor -- Kjendal

JUDGE MCNAMARA: No. No, just that it's spelled K-J, and I do kind of pronounce as little --

MR. HANNAH: Yes, I mean, call it -- we can call it KJ, but -- so KJ does not disclose that at all. KJ is talking about -- let me back up. What is KJ talking about? KJ is talking about a system in which you want to identify applications. So you'd send this to an application identifier, but this isn't -- we're not talking about, you know, application level protocols, things of that nature. It's like applications that data might be coming from. And then it also teaches that you have this mirroring technology, and the mirroring technology is used, you know, throughout the context when you read all 32

columns of KJ, it specially talks about how you can use this mirroring technology to send it to the application identifier. Now you can have various criteria that you're going to be able to do that.

The problem with it is that you don't mirror in response to a packet transformation function. It doesn't talk about that at all. The mirroring is done to send it to an application identifier. That's what the mirroring is done for. Now, there is a line in there that says you're going to send it to a network logger, but again that's too late. It has to happen before the mirroring if you're going to follow the Petitioner's argument, because the packet transformation function, it's in response to. The in response to the packet transformation function is what the routing has done. So the mirroring is not in response to sending it to a logger. The citation that they cite which is, you know, extremely limited, cited multiple times. It does say it, but it says that you can mirror to a network logger. It's backwards. Even if it was the right way, even if it did come before, it doesn't talk anything about the packet transformation function that's detailed in the claims.

If you try to combine them, what do you get? Well, according to the Petitioner, you're going to have several elements that are going to be met by ACNS. So you're going to have a transaction log, and then it's going to be mirrored to a logger. Why would one of skill in the art do that? I don't know. It's not in the Petition and it's not in the reply. There's actually no indication why you would do a transaction log which I think I've stressed enough is multiple packets, and, it, I mean actually has nothing to do with packets; it has to do with application layer, but a transaction log -- and then I'm going to mirror that and then send it to a network logger. It doesn't make sense. It doesn't make sense to do it in that way.

So there's simply -- and, I mean, and I say that when the only thing that they rely upon, though, for this limitation is the KJ reference. They don't have anything else in the Petition. It's KJ. It says KJ can be combined with other things, but for that limitation, when you look in the Petition, it's KJ, so the in response to has to be in KJ and it's just simply not there.

Your Honor, did you have any -- I'm trying to look at the camera in front of me instead of the monitor. And it might be looking weird to you, but are there any questions, Your Honors, in terms of the KJ reference or the combination, because I'm going to move back to some kind of earlier elements in the claims that I think kind of get more in the weeds, but -- no? Okay.

JUDGE MCNAMARA: Don't worry, we'll interrupt you.

MR. HANNAH: No. Yes, very good. Yes.

JUDGE MCNAMARA: It's what we do.

MR. HANNAH: I love that. As you know, I appreciate that. All right, so let's talk about -- I think it's worth discussing the security aspects. I do. I think it's important to point out that there is no security aspect of ACNS. They point to the word "security". I see it. The word "security" is in there. But when it's talking about security, it's talking about authentication. It's definitely not talking about packet level security which is what the 213 Patent is about, a packet security gateway. It's absolutely not talking about analyzing each packet in order to secure a network which is what this is, the packet security gateways in the claim specifically do.

JUDGE MCNAMARA: So you use the word "authentication". By authentication do you mean that the message is what it says it is?

MR. HANNAH: No, it's what the users who says it is.

JUDGE MCNAMARA: Okay. The users who says that it is.

MR. HANNAH: Yes. So, and when you look at ACNS, it's very specific in that when you do authentication, they're looking at -- and this actually goes right back to the argument that we're looking at transactions, the whole thing. You have to have the user information in there, in the transaction in order for the authentication to even happen so that you can have the content come back. So one of the fields when you actually look in the transaction logs that you can put in in the customized fields is the user. It's the user name. Again, showing that this is the transaction that's happening across the proxy. It can't be packet going in, packet going out. It just has no notion of that. But it's the authentication of the user. That's what it's talking about in the security based on that.

The Claim 1, and I'm just showing the -- in my demonstratives, Your Honors, but I'm just showing, you know, Claim 1. We talk about packet security gateways that are associated with the security policy manager. It's talking about providing packet level security for these things, and it's just not simply in ACNS. It doesn't need to have it. This turns me again to Fuchs. It's in Fuchs? Fuchs. And this is the part that it got contested in the surreply, and I know, Your Honor, during the prehearing conference you said, "Assume that the motion to exclude". I mean, essentially you said. You know, I hate to characterize what Your Honor says. My understanding is that, you know, we're supposed to address it like the Fuchs Supplemental Declarations and --

JUDGE MCNAMARA: Well, if it were. Yes.

MR. HANNAH: If it were, then, yes.

JUDGE MCNAMARA: Well, right. Because we will not have ruled on it by today.

MR. HANNAH: Right. But, of course, you stated it better than I could, so the -- if it were ruled on. So I'm assuming that it's in. Assuming that it's in. I don't think it should be in, but assuming that it's in, we have contrary testimony from Mr. Fuchs in terms of the security. Here on Slide 13, we asked him, does the content engine perform any security analysis on the request? And he specially says, "The content engine does not perform any inspection of data within the object. No." And we follow up, to be specific, does it perform any security analysis on the request itself? If the request does it, yes, it's to repeat. It does not.

I think that's clear testimony.

What does he say in the supplemental declaration? Well, in the supplemental declaration, he says, "Well, I was mistaken. I looked through the manual. It does talk about security. What you see, though, is he does not recant the information about the security analysis performed on the request. He says it mentions the word "security". It does; it mentions the word "security". That's security for authentication. Again, a higher level, application layer level authentication for a request in content, request in content for the origin server or for the cache, but this higher level authentication.

He never comes back and says that it does a security analysis on the request itself. Any security analysis that could be done on a packet basis to protect a network at the packet level, and when we're talking about packets, as I started out, we're talking about layer 2/layer 3. It's simply not there, and that part of Fuchs is unrebutted as well.

Now, if you wanted to talk about the DiffServ. DiffServ is found in Claim 10. Oh, well, I'm sorry. Your Honors, any questions on the security aspect or arguments? I think that's actually laid out very clearly in our

briefing. Once you go through that, you'll see it when we talk about security and talk about how (inaudible) that's really talking about authentication. All right.

Claim 10. Claim 10 is different than Claim 1. It has this DiffServ element in it, and an additional reference is introduced by the Petitioner to show that this limitation is in there. Again, there's no disclosure of how this DiffServ is going to work on a packet-by-packet basis combination with ACNS. It's simply absent. And there's absolutely no disclosure of DiffServ and using it for security. I'm showing Slide 19, Your Honors, in Texas, of our slide deck. In terms of DiffServ and, well, you know, what is it showing, and it's showing that the DiffServ is showing about packet classification, but it has nothing to do with packet identification criteria, and it has nothing to do with security at all.

I think that's clearly laid out in our briefing, but I think it's worth noting in that this additional limitation it needs to, in addition to all the arguments that I just raised, has to show that it's going to fit into this kind of security realm and on a packet-by-packet basis and with these dynamic security policies, and when you look through that reference and you look through how the combination is, there is no indication in terms of how it's going on apply for security.

And since I've got time, might as well use it, you know, one point that we did make in the -- and in it's our slide deck, too, but, you know, I'm highlighting this, what I think is just the simple arguments, but, you know, when we do talk about the dynamic security policy and we do talk about how the security policy manager has to be able to send a security policy to the packet security gateways, I think there is a distinction between an administrator getting on and, you know, typing in one rule over another

versus what the claim is requiring, which is saying that you're going to be sending a policy to the packet security gate which I know we covered this ad nauseam and in other hearings, but I think it is worth repeating when you -- and that's another thing that I gathered from the prehearing conference which said you can repeat, but we have heard this stuff before, but it does specifically say that you receive by each of those packet security gateways a dynamic security policy, and the only disclosure that they're showing there is an entry that's done by a manager that's going to be pointing to the content engines which is again these web proxies, these cachees, and sending those just being able to do that on that command line interface, I don't think is showing what -- and this is throughout our briefing.

All right, so I've got five more minutes, it looks like, and I will hit the secondary consideration. I mean, objective indicia of non-obviousness. I don't like calling them secondary considerations for obvious reasons when I'm representing the Patent Owner. If I was on their side, I'd probably call them secondary all day long, but for objective indicia of non-obviousness, you know, Judge White has hit me a hundred times before on this issue in terms of where is it? Where are you talking about the nexus? Where is it in here?

Okay, Your Honor, I'm pointing to the same evidence that I pointed to before which is the ESG whitepaper and the other evidence that's cited and specifically here, you know, I pointed out the highlighted stuff before, but I also want to point out that, you know, it talks about dynamically monitoring for these advanced threats using this intelligence and it specifically talks about how you can use these indicators to drive actions such as logging, and I'm going to, you know, have to obviously rest on what I've put into our papers, but, you know, a secondary consideration, you know, Centripetal

Technology is important and it's important because it does a lot of these features, and I know we've got a lot of patents, you asked, Your Honor -- I mentioned this in the beginning -- how many patents do we have that are addition in terms of the IPR-7 patents that have been instituted.

JUDGE MCNAMARA: Okay. The reason why -- I think we talked a little about this during the prehearing conference, too, that it's always difficult.

One of the most difficult things that a Patent Owner has to do when he's trying to raise the issue of objective considerations is connect the nexus between the claimed subject matter and the long felt need, whatever publications there are and all that sort of thing. I guess what I'm -- you know, have the success of the product and that sort of thing, but when you have seven patents that we have here in dispute, and I guess there are more patents that are not in dispute on this subject matter on this product, right?

MR. HANNAH: Correct. So I've got nine patents total, 14 petitions were filed, we have 9 IPR trials, and that's on 7 patents.

JUDGE MCNAMARA: So what I'm wondering about (audio word drop) the industry recognition, the praise, that sort of stuff, when it's spread over subject matter of seven patents, it seems very difficult to connect that kind of recognition to the claims of any one patent. And I was wondering if you had had any thoughts or had done any research on that issue. I mean, that, you know, well, there's seven patents out here and, you know, no one's going to write about all this, well, you know, because they don't know what we're claiming --

MR. HANNAH: Right.

JUDGE MCNAMARA: -- so there's seven patents out there, and no one's going to write on just, you know, connecting elements to one patent,

but we've got a lot of patents and we've got a product out there. So how do we adjust for that in the standard when we're trying to figure out what a nexus actually really is?

MR. HANNAH: It's a great question. I'm familiar with the case and all this says the nexus is presumed, and we go through that (inaudible) in our briefing for all of these different cases that it is presumed and certain circumstances I think we meet that threshold. And what Centripetal has done is it does have multiple patents on these multiple technologies generally related to security, you know, providing security at the packet level. I mean, there's, you know, some claims, yes, have different things, but this is what we're, you know, talking about for this case at least.

But I don't think the fact that, and this is a question from Judge White, actually, that if you have multiple patents and you're showing similar evidence that that, you know, kind of, you know, waters out all, you know, the evidence for everything. I think that you do have to look at -- holistically you have to look at it as a whole and see, okay, you know, in light of -- I mean, we have the case all with the next presumed, but in light of what are they talking about here, and when you read it in detail it's talking about, okay, we have these large amount of rules that we can process.

This is maybe for some other patents. And we can do this capability at extremely fast speeds and -- you know, which is some elements in some other patents -- and then we have this logging capability in order to be able to, you know, make adjustments and see what needs to happen. I think all those, and you're looking at a whole, that's what you have to consider, but the specific point about I've got seven patents, and then, you know, how did that weigh into the analysis; I think we're going to have to make a new law on that one, Your Honor.

JUDGE MCNAMARA: Well, and it goes to Judge White's question from last time, though, about, well, does it water it down, or do we have to look at it differently?

MR. HANNAH: I think you have to look at it differently. I think you have to look at it as a whole for each case. I mean, you can't ignore that (inaudible) can I ignore it? No, you can't ignore it. I mean, this is our position. I'm going to put it out there every time and stand by the position, so you can't ignore it, but I don't think it -- because I did think about that afterward. It doesn't water it down. The fact that you have some more evidence or the same evidence for multiple patents, if you can show, you know, where you need the nexus, assuming it's not presumed, what are the different elements and things like that, and as a whole is that's what it's trying to teach. I think you have to look at it case by case. Of course, you have to consider everything, but you can't say, okay, well, they used this evidence over here, now it's watered down for this, and so --

JUDGE MCNAMARA: Yes, I guess that's the point. I mean, you get this glowing article about how successful a particular product is and then you find, well, I want to use it here, but then I use it again for -- you know, I've got six other patents, and does it help or hurt?

MR. HANNAH: You know my position. It helps.

JUDGE WHITE: I think you put it another way. Is there a different framework we need to look at when we've got this multi-patent situation? I think the other patent we looked at the last time was with the 552, so let's just say the 552 was something that people really -- the claim saw something people really bought in to, does that change the analysis when we're looking at here this, I think 213, to see, you know, what is it that people are drawn to, and since they're all your patents, how do we look at this holistically;

what is sort of the framework for this multi-patent situation in a singular product?

MR. HANNAH: Right, and, you know, it comes down to when you look through these articles and it talks about how you're operationalizing this threat intelligence. You're doing it on this very fast basis, packet-by-packet, and I think that you see that all of these patents are kind of different pieces of the puzzle in terms of how to do that. You know, like you have to have the preprocessing of the rule sets in order to, you know, have different aspects of that, and that addresses kind of the praise that we're getting here as well, that, okay, we can be able to process multiple rules in order to -- and then you have where I can do this logging on a packet-by-packet basis at these extremely high speeds and, you know, loggings capture it, so I think it's all these different pieces form this product and, you know, we try to highlight as best we can the different pieces and how they're highlighted in all of the publications as well, but I don't know if that helps in terms of the framework or, you know, it makes it more confusing --

JUDGE WHITE: I guess I'm thinking about sort of like, do we look at it and if we see a feature that we think is particularly important as long as it's covered by a patent then it's not a problem for anyone to know their case, but if we see that, okay, this particular feature that seems to be getting particular praise doesn't seem to be covered by any of the patents, then they've got a problem. Is that what we need to be doing, looking at these features and saying, well, is there a patent in this group that that feature is tied to, and if so, is it just the patents that are in litigation in front of us now or is it your whole portfolio, and if it's your whole portfolio, how do we know?

MR. HANNAH: Right. Right. Yes. They're all very good questions. That's why I'm not a judge.

JUDGE MCNAMARA: It must be if we have the answers.

MR. HANNAH: So, I think --

JUDGE WHITE: But it means you get to chime in.

JUDGE MCNAMARA: Yes, you get to tell us.

MR. HANNAH: I think my chime-in on that is that I think you have to look at -- I think you do have to look at the features; I think you do have to look at the praise and the problems that holistically it's trying to solve, and that those -- you know, it's not like these patents are solving -- they're all related to the same product that's doing the same operation and things like that. It's not completely, you know, different fields or anything of that nature, so I think when you look at it holistically like that, my take is that, you know, you kind of have to look at what is the product doing and how is it doing that, and if that product is successful for certain features, then you take that all into account and find that all the patents are not obvious, so.

JUDGE MCNAMARA: All right, thanks very much.

MR. HANNAH: Thank you.

JUDGE MCNAMARA: You have 11 minutes left.

MR. HANNAH: All right, thank you.

(off the record.)

MR. BLAKE: So, Your Honor, I'd like to, I guess pick up quickly where we left off. Judge White, to your question, as this is a complicated -- and yours, too, Judge McNamara, it's a complicated situation where you have multiple patents, but respectfully it does water it down some, right, because the question really is, is the commercial success really due to any number of seven patents? Is the industry praise due to any number of seven

patents? I mean, presumably they all cover separate subject matter, although as there wouldn't be seven patents, and while this is a tough area of the law, there's a check on the system that is at least one way that they address this which is to say you have to prove that the product, because you don't want an unnecessary presumption -- you have to prove the product is coextensive with the claims or at least that it's practicing the claim elements, and separate and apart from the point of whether it's watered down what you have here is no real proof that it's practicing the claim elements.

I hear my colleague talk about the fact that the ESG article which they commissioned does reference logging. Well, throughout the course of his argument he was hammering on the fact that the claims say that logging requires identifying a subset generating a record, reformatting. Well, none of that discussion is in the objective indicia section. They had the opportunity. They have the knowledge with their people to say, look, this is how our products identify a subset, generate a record, reformat it. This is how they route it to a monitoring device. There could have been a declaration that established all of that and shown that it is coextensive with the claim language, but none of that's there.

The ESG article, all it does is say, "logging". That doesn't mean that it's the logging that's claimed in the patents. So it'd be completely inappropriate to apply that general vague statement and say, okay, now we have a nexus. Something more has to be required in that situation.

JUDGE MCNAMARA: You mentioned that they commissioned the ESG article. What was the circumstances there? I don't remember.

MR. BLAKE: Oh, sure. Let me see if I can pull up the issue. It's on the first page. It's at the bottom of the first page. It says, "Commissioned by Centripetal Networks." I apologize, but I don't have it handy.

JUDGE MCNAMARA: No, that's perfectly fine. I just didn't recollect that detail. That's (inaudible).

MR. BLAKE: Yes, it says it on the bottom of the first page.

JUDGE MCNAMARA: Okay. And so that makes it perhaps less weighty.

MR. BLAKE: Less weighty in my mind. Yes. That's a nice, good word for it. Let me try to step back, and I apologize. I'm kind of jumping around a little here, but some of these arguments are kind of coming up for the first time, and I would say some of them, I would beg, where are they even in the papers?

JUDGE MCNAMARA: Well, I had some of them in response to our questions, too, so.

MR. BLAKE: Sure. That's fair. But one of the things that I hear is that ACNS has no reason whatsoever to consider network layer packets because it talks about HTTP requests and therefore that must mean we're only talking about application level information. Well, respectfully, as a starting point, the patent doesn't think of it that way. All right? I mean, the patent -- and I'll go back to my reference to Claim 5 earlier, the patent talks about HTTP requests and a GET method just like ACNS does, and the patent is talking about the fact that you may look at a particular HTTP request, but you are going to do processing even though that's the language, HTTP packets, HTTP GET method call. That's the language of application layer packets, but it is Patent Owner's contention, and we agree that the patent is talking about an analysis of layer 2/layer 3 packets, specifically because the application layer packets are embedded within those network layer packets, and we are talking in a security analysis, and how are you performing the security functions as opposed to the content functions?

When you're talking about the security layer, just because you're talking about the request method isn't not mutually exclusive with looking at a network layer packet. That's what's done in the patent; that's what would be done in ACNS. When Patent Owner raises this argument that says, you know, ACNS is talking about, you know, the fact that you'd have to reassemble to do stuff, even in their own surreply, all they're talking about is that the reassembly in the content engine would be done for the content delivery analysis. It's not required that that reassembly be done for the security analysis. The packet can come into the content engine. I think we saw Figure 1.2 of Exhibit 1008 before it comes into the content engine, it comes out of the content engine. It comes in as a packet; it comes out as a packet.

The security analysis can easily be done on a packet-by-packet basis, and Dr. Jeffay, no one has said that it can't be done on a packet-by-packet basis. A matter of fact, I'd cite to Dr. Jeffay, Exhibit 1020, paragraphs 32 and 33, and 39 and 40 as examples of Dr. Jeffay saying I hear their argument about reassembly, but that's not required for the security analysis to take place, and so I respectfully would say, what we have to do is we have to separate here how are you working on the content and provision of content and how are you doing the security. No one denies; I wouldn't deny that ACNS is about content delivery.

There's a lot large portion of it about content delivery, but respectfully there is a security analysis component that is significantly involved in ACNS, and that is shown -- let me pull it up here -- our Demonstrative Slide 17 which talks about -- Exhibit 1008, page 1-9, it talks about what's going on, and it makes two different references to system security.

The first one says, "Authenticate monitor log and control web access from end-users to implement corporate policies regarding work environment and system security." Now, authentication is one part of that, but so is monitoring and other types of system security. Later on further down the page, there's an example of system security that's used. This example wasn't mentioned at all by Patent Owner, but it talks about system security trying to stop viruses such as Code Red, so the system security, what's being done, is not limited to just authentication. The system security is broader than that.

And particularly as we get to the time of the invention, when you get to the 213 Patent you would understand that system security requires even a broader scale of things because a person of ordinary skill in the art reading ACNS saying it can do system security would not be limited to just using the system security that's disclosed in ACNS. It's what he or she would understand at that point in time. And the fact that it's broader than authentication, that it talks about viruses as another type of system security teaches you that you have to think boarder than just the authentication context, and in that respect, it's not just that ACNS is geared towards webmasters who are trying to impellent just the webpage.

ACNS says it's geared towards administrators who may have to have some of the knowledge of a webmaster, but it does not limit ACNS to just the use by webmasters. Indeed other layers of packet information are discussed and you'll forgive me because we haven't in the papers gotten into an argument before about whether or not there's any discussion of network layer packets as opposed to just application layer packets, but I would cite to ACNS pages 4-13 and 4-24 as discussion of layer 2 packets that's being evaluated by the ACNS system. It's not that it's limited entirely to what's going on in an application layer packet because the subject matter is not

limited entirely to the delivery of content. It also includes the delivery of application layer packets in network packets and how you are going to apply network system security to that.

Now to get to the point of identifying a subset of information and the specific examples that we cited, first when talking about the packet-by-packet analysis, let's go to this identifying step that my colleague focused upon, and, again, we always go back to the claim language. What does the claim language say: Identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application layer packet header information. Again there's no question that the log entry -- that we cited both log entries that we cited are talking about packets that are less than 1,500 bytes, so those packets could -- the request, itself, the response, itself, it could fit within one packet.

The information that is the subset of information specified by the packet digest logging function is not necessarily restricted to only information that's in the request or the response. You could look and identify other information such as for instance that apache-style squid log, the one that has the 632 bytes. I'll use it. We have limited time, but I'll use it as an example. And let me pull it up. It's our Demonstrative Slide D20. There is no doubt that you are looking at a request about a GET -- this is a GET request. This is a GET request just like what you see claimed in Claim 5 of the 213 Patent. This is a log about a GET request, the GET, the size. They don't question that that size is less than the 1,500 bytes.

The only argument I heard in this particular one, and we can get to the others, is a brand new argument that you'd find nowhere in the papers that this 200 indicates the response state. Well, even if that response state wasn't in the GET request, itself, which it wouldn't be, that can be information

about the packet that is being logged as far as what is the response state on this particular request. It's not required that that subset of information come from this packet, itself. The claim language in the 213 Patent just doesn't say that. I'll make two other points and then cede my time, to the extent I have any.

Number one, with respect to the routing limitation. Again, the focus was in the wrong place because we're talking about is it in response to the packet transformation function reading the claim language as if the packet transformation function that you're acting in response to has to be a digest log. But that's not correct. That packet transformation function claim language, if you go back to Element 1.1, it's defined with a comprising. I mean, Claim 2 shows the packet transformation function can be broader. It can include a forward, and how it's happening in Kjendal, KJ or however we want to call it, is you are mirroring what is the routing to a monitoring device, the logger or an IDS. You're routing it in response to the forward transformation function.

There is some evaluation of the application layer information according to a policy, and then there is a decision made to forward it, and in response to that decision, it is forwarded, so it is in response to a packet transformation function as that term is contemplated by the patent. That's what Kjendal is teaching. The forward is the packet transformation function. It's routed in response. That's how it works. It's directly analogous.

And finally I'll talk a little bit about Claim 10 because I didn't when I first stood up, but Patent Owner brought up Claim 10, the DSCP. No one challenges the fact that all these references talk about the use of quality of service and the DSCP and how that works. What the argument strictly goes, and it kind of ignores the whole of ACNS, it says, "Well, it never mentions

its use for security purposes." ACNS is about security, and ACNS teaches, and the DiffServ in combination teaches that you can use qualify of service to treat different packets differently. And a person of ordinary skill in the art, it'll be plainly obvious to them that if I'm implementing security and I have security problems, and it's caused, by say, a DOS attack, then I'm going to treat the packets that appear to cause my DOS attack differently. I can use that quality of service to bring up and start allowing packets that don't appear to cause a problem and quarantine or drop the packets that do appear to cause a problem. I mean, that by the 2014 timeframe, DOS attacks unfortunately were so rampant that this would be as trivial a step as could be. With that, if there are any questions?

JUDGE MCNAMARA: All right. Thank you very much, Counselor.

MR. HANNAH: So, Your Honors, I think I've hammered home my points with regard to the transaction log and the proof that's actually pointed out in the Petition and the reply and how the arguments made in the Petition and the reply are that that is a single packet and it's impossible to do so. One point that was raised on the rebuttal, there, was that the -- I believe he said that there is no disagreement in terms of the size and what that's referencing. If you look at it, and if you look at what the squid log is showing, when it shows the 1,100, it's after the -- I'm looking at 19-1. I'm looking at the squid log format. It says, "Time elapsed, remote host, code status bytes."

That 1,100, I'm pretty sure, is the GIF that comes back. That's the GIF file. That's not showing what the size of the request is going out. That's the content coming back, is at news.GIF. I mean, I'll concede. I'm not sure if that's in that specific statement. This is in response to his statement, but that GIF file is the content coming back. And so at the very least, I want to say that there's no agreement saying that we think that that's the size of the

request coming out. I've already pointed out how that transaction is a complete transaction at the HTTP level.

Another point that was made on the rebuttal, he pointed to the virus, the Code Red, and it's not up there, and he said, okay, well, this shows that it kind of that deals with security. Well, it actually says how it deals with that. If you look at 16-1, ACNS is pretty clear. So let me back up. I think we're all aware that a virus is going to come in the response, right? It's going to be in the content that comes back. And so I don't think they're talking about a request that contains a virus, of course not, but it's talking about the response. So if you go to 16-1, it talks about what you do for virus scanning, and the content engine doesn't do any of it.

It says, "ICAP is an open standards protocol that can be used for content adaption typically at the network edge. Content adaption includes virus scanning, content translation, content filtering, content insertion, and other ways of improving the value of content to end-users, and it talks about how you do it. ICAP specifies how a content engine acting as an HTTP proxy server can communicate with an external device that is acting as an ICAP server which is the one that filters and adapts the requested content. It's not the content engine that's doing any virus scanning. It's the third-party device that it can integrate with. And it makes sense. It's a proxy. As a proxy, it's going to communicate with a third-party device in order to do any type of virus scanning, so the virus scanning that's been talking about in the ACNS reference is not done on the content engine. It's actually done on another device.

I think, well, the final point that Counsel made was about the in response to and the packet transformation function. Again, the packet transformation function that is identified is the wrong packet transformation

function. Forwarding is not the packet transformation function that's set forth in the claims. It has three specific steps. It talks about identifying, generating, reformatting. That's the packet transformations function. So when it says that in the class element, it has to be in response -- you route in response to the packet transformation function. It's the packet transformation function that contains those three steps. It's not just merely forwarding.

And that's my point that I was trying to raise when I talked about KJ, is that it doesn't have the packet transformation function and there's no disclosure. It's completely absent from the record in terms of the packet transformation function that's the -- routing that's done in response to the particular packet transformation function in the claims. Unless there's any questions, I will sit down and wish everyone a happy holiday. I'm sure you've seen enough of me for the last month, so I hope you all have a nice holiday and we'll see you in the new year.

JUDGE MCNAMARA: Yes, I think that's right. Okay, Counsel. All right, we'll take the case under advisement at this point. I hope you all do get a chance to get a little rest over the holidays, and I'm sure we'll be back, but as for now, this hearing is adjourned, and thank you all very much.

(Whereupon, the oral hearing at 3:01 p.m. was concluded.)

PETITIONER:

Daniel McDonald
Jeffrey Blake
Kathleen Ott
Michael Wagner
Christopher Davis
MERCHANT & GOULD P.C.
dmcdonald@merchantgould.com
jblake@merchantgould.com
kott@merchantgould.com
mwagner@merchantgould.com
cdavis@merchantgould.com

PATENT OWNER:

James Hannah
Jeffrey Price
Michael Lee
KRAMER LEVIN NAFTALIS & FRANKEL
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com

Bradley Wright
BANNER & WITCOFF LTD.
bwright@bannerwitcoff.com