

Transcript of the Testimony of:

DR. MICHAEL FRANZ

NETSKOPE, INC.

VS.

FORTINET, INC.

December 28, 2023

Volume I



I M A G I N E
R E P O R T I N G

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,
v.
FORTINET, INC.,
Patent Owner.

PTAB Case No. IPR2023-00459

Patent No. 10,084,825

REPORTER'S TRANSCRIPT

DEPOSITION OF

DR. MICHAEL FRANZ

Thursday, December 28, 2023

Via Zoom Video Conferencing

10:02 a.m.

Reported by: Rachel N. Barkume, CSR, RMR, CRR
Certificate No. 13657

A P P E A R A N C E S

FOR THE PETITIONER:

PERKINS COIE LLP
By: ANDREW KLEIN
BINGJIE (KAY) LI
Attorneys at Law
11452 El Camino Real, Suite 300
San Diego, California 92130
(858) 720-5700
aklein@perkinscoie.com
bli@perkinscoie.com

FOR THE PATENT OWNER:

QUINN EMANUEL URQUHART & SULLIVAN LLP
By: OGI ZIVOJNOVIC
QUINCY LU
Attorneys at Law
865 South Figueroa Street, Floor 10
Los Angeles, California 90017
(213) 443-3251
ogizivojnovic@quinnemanuel.com
quincylu@quinnemanuel.com

I N D E X

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

PAGE

EXAMINATION BY MR. ZIVOJNOVIC

4

EXAMINATION BY MR. KLEIN

74

--000--

E X H I B I T S

EXHIBIT

PAGE

Exhibit A Institution Decision by Patent Office 18

Exhibit 1002 Declaration of Dr. Michael Franz 24

Exhibit 1001 United States Patent No. 10,084,825 29

Exhibit 1004 Chandra Patent Application 39

Exhibit 1008 Keohane Patent Application 57

Exhibit 1005 Buruganahalli Patent Application 72

1 BE IT REMEMBERED that on Thursday, December 28,
2 2023, commencing at 10:02 a.m. thereof, via Zoom Video
3 Conferencing, before me, Rachel N. Barkume, a Certified
4 Shorthand Reporter in and for the State of California,
5 remotely appeared from Irvine, California,

6 DR. MICHAEL FRANZ,
7 a witness called on behalf of the Patent Owner, who,
8 having been first duly sworn by me to testify the truth,
9 was examined and testified as follows:

10 EXAMINATION

11 BY MR. ZIVOJNOVIC:

12 Q. Could you please state your full name for the
13 record.

14 A. My name is Michael Franz, and I have two middle
15 names, Stephen Oliver, that I don't usually use on my
16 publications.

17 Q. And I would like to go over some ground rules
18 before we get started. You understand that you're under
19 oath to tell the truth today.

20 Do you?

21 A. Yes.

22 Q. The court reporter is creating a written
23 transcript of today's deposition. To create a clear
24 transcript, one important rule is that you let me finish
25 my questions before responding, and I will let you

1 finish your answers before asking the next question.

2 Agreed?

3 A. Yes.

4 Q. It is also important you give verbal responses
5 to my questions rather than nodding or otherwise
6 answering nonverbally.

7 Agreed?

8 A. I'll do my best.

9 Q. At some point I may ask a question that you do
10 not understand. If I do, please let me know. I'll be
11 happy to rephrase or to try to clarify.

12 Agreed?

13 A. Yes.

14 Q. If you answer my question without asking for
15 clarification, however, I will assume you understood it.

16 Agreed?

17 A. I'll do my best.

18 Q. Is there any reason at all why you cannot
19 provide full, true, and accurate testimony today?

20 A. I'm not aware of any reason.

21 Q. You understand that this deposition is in
22 connection with an IPR relating to U.S. Patent Number
23 10,084,825; right?

24 A. Yes.

25 Q. Is it okay if we refer to this as the '825

1 patent?

2 A. Yes.

3 Q. Now, you analyzed the '825 patent; correct?

4 A. Correct.

5 Q. And you submitted a declaration regarding the
6 invalidity of the '825 patent in light of certain prior
7 art; correct?

8 A. Correct.

9 Q. One of the claim terms in the '825 patent is
10 "cooperative security fabric"; right?

11 A. Yes.

12 Q. And in your declaration, you opined that you
13 found that the prior art discloses such a cooperative
14 security fabric; correct?

15 A. Yes.

16 Q. Fair to say, then, that you understood the
17 scope of the claim term "cooperative security fabric"?

18 MR. KLEIN: Object to form.

19 THE WITNESS: What do you mean by "scope"
20 exactly, please?

21 BY MR. ZIVOJNOVIC:

22 Q. In analyzing the prior art, you applied a
23 certain meaning of the term "cooperative security
24 fabric"; right?

25 A. So we did not construct this term "cooperative

1 security fabric," so I used the plain and ordinary
2 meaning of the term "cooperative security fabric."

3 Q. And is it okay if we occasionally use "CSF" as
4 an abbreviation for cooperative security fabric?

5 A. Yes.

6 Q. So you agree that cooperative security fabric
7 has a plain meaning, then?

8 A. Well, so the word "fabric" is a well-known term
9 in the art, and, you know, the word "cooperative" is
10 clear in this context, and the word "security" is, you
11 know, clear that we're talking about the parts of the
12 fabric that are having security functions. And so I
13 believe that a person of ordinary skill in the art at
14 the time would have understood what is meant by this
15 compound cooperative security fabric term.

16 Q. What is the plain meaning of fabric in the
17 context of network and data security?

18 A. So a fabric is the physical structure of a
19 network, so the topology of the network. So, you know,
20 which -- which part of the network is actually directly
21 connected to which other part of the -- what is the --
22 the physical layout of the interconnectedness and where
23 are these parts located.

24 Q. Now, is the word "fabric" -- let me start over.
25 You understand the word "fabric" is a reference

1 to clothing fabric; right?

2 MR. KLEIN: Objection. Form.

3 THE WITNESS: So, I mean, I understand that
4 somehow the -- the use of the term in computer science
5 and networking actually sort of may be inspired by the
6 idea that you have cables weaving, you know, through
7 buildings and such. So that's probably where the
8 analogy comes from.

9 BY MR. ZIVOJNOVIC:

10 Q. So you would agree, then, that at a minimum,
11 the word "fabric" in the context of network and data
12 security is inspired by the phrase "fabric" in the
13 context of clothing; right?

14 MR. KLEIN: Object to form.

15 THE WITNESS: I don't know one way or other.
16 This is anecdotal. I just -- I just know that the term
17 "fabric" to refer to the physical infrastructure of
18 networking was in use at the time and is still in use.

19 BY MR. ZIVOJNOVIC:

20 Q. So sitting here today, it is your understanding
21 that the term "fabric" in computer science and
22 networking was inspired by the idea of threads weaving
23 in clothing; right?

24 MR. KLEIN: Object to scope -- or sorry, object
25 to form.

1 THE WITNESS: So as I said, this is anecdotal.
2 I'm -- you know, I'm not historian of computer science
3 terms. I would -- you know, that is -- I'm aware of the
4 term, I've been aware of the term for a long time, but
5 that is a guess. I have no way of scientifically
6 establishing whether or not that term comes from
7 clothing, but it's an educated guess. I don't think it
8 really matters where the term comes from.

9 BY MR. ZIVOJNOVIC:

10 Q. Now, a piece of clothing fabric is made up of
11 many threads; right?

12 A. Probably.

13 MR. KLEIN: Object to scope.

14 THE WITNESS: Yeah. I'm not an expert on -- on
15 clothing, I'm afraid.

16 BY MR. ZIVOJNOVIC:

17 Q. I'm just asking your understanding of the plain
18 meaning of these words.

19 Is it your understanding that the plain meaning
20 of clothing fabric means that it's made up of many
21 threads?

22 MR. KLEIN: Object to scope.

23 THE WITNESS: As I said, I'm not an expert in
24 clothing. I can tell you that the plain meaning of
25 networking fabric is the cables and boxes that make up

1 the physical infrastructure of your network.

2 BY MR. ZIVOJNOVIC:

3 Q. What is a computer network?

4 MR. KLEIN: Object to form.

5 THE WITNESS: So a computer network is the
6 infrastructure that connects computers to each other.

7 BY MR. ZIVOJNOVIC:

8 Q. And what is a network topology?

9 A. A network topology is the abstract -- the
10 abstract thing that tells you which -- which part -- who
11 connects to whom. So you could have a computer that is
12 directly connected to lots of other computers.

13 You could have, like, one thing in the middle
14 that directly connects to everyone; that's called a star
15 topology. Or you could have a -- everyone could be
16 connected to everybody else directly; that's called a
17 crossbar. Or you could have more complicated
18 arrangements where in order for one person to talk to
19 another, you would have to go through intermediaries.

20 And so the topology tells you who is connected
21 to whom directly.

22 Q. Is it fair to say that every computer network
23 has a network topology?

24 A. I think that's fair to say.

25 Q. And in your view, does every network topology

1 qualify as a fabric?

2 A. So I think the fabric is -- is one level below.
3 Right? The fabric is how do you physically realize the
4 topology. So that -- how do you -- how do you -- what
5 box is, you know -- what cable, what box, what other
6 things are in between, how are these things plugged
7 together. And the physical things that do this
8 connectivity is the fabric.

9 Q. Would you agree that every computer network
10 requires some form of physical connectivity between its
11 constituent computers?

12 MR. KLEIN: Object to form.

13 THE WITNESS: Well, you could have wireless as
14 well, right, so -- you could have wireless links in your
15 network.

16 BY MR. ZIVOJNOVIC:

17 Q. If computers are in a wireless network, does
18 that mean they lack a fabric?

19 A. No. The fabric would contain, you know, the
20 wireless antennas and base stations and those things.

21 Q. Let me rephrase my earlier question to clarify
22 that point.

23 Would you agree that every computer network
24 requires some form of physical connectivity, wired or
25 wireless, between its constituent computers?

1 A. Yeah, so every -- in order to create the
2 network, you need some form of connectivity.

3 Q. In that case, would you agree that every
4 network has a fabric?

5 MR. KLEIN: Object to form.

6 THE WITNESS: So I do not believe that for
7 very, very simple, you know, just two things plugged
8 together, you -- yeah, the word -- I mean, fabric,
9 meaning the physical structure of your network, yes.

10 So networking requires a physical underlying
11 connectivity infrastructure, and that is the fabric.

12 BY MR. ZIVOJNOVIC:

13 Q. Are you familiar with IEEE 802.3?

14 MR. KLEIN: Object to scope.

15 THE WITNESS: There's a lot of 802s. Which one
16 is dot 3?

17 BY MR. ZIVOJNOVIC:

18 Q. Would it help if I reference that it's --
19 relates to ethernet?

20 A. Okay. So 802.11 is the one that's wireless
21 that everyone knows the abbreviation. So I'm familiar
22 with ethernet. I'm not familiar in every detail with
23 the standard.

24 Q. Would you agree, though, that 802.3 is a
25 standard -- let me start over.

1 Would you agree that ethernet is the standard
2 for networking computers together?

3 MR. KLEIN: Object to scope and form.

4 THE WITNESS: So ethernet is a connection
5 technology that can be deployed within a network.

6 BY MR. ZIVOJNOVIC:

7 Q. And you're familiar, right, that I can connect
8 two computers directly via an ethernet cable; right?

9 A. I have done that myself, yes.

10 Q. And when you connect two computers together via
11 an ethernet cable, they communicate with each other
12 using the ethernet standard; right?

13 A. I'm sure you could rig up solutions where
14 you're communicating via the existing physical ethernet
15 cable using other standards, but -- but, you know, one
16 of the ways that you could communicate by having two
17 computers connected in that way would be via the
18 ethernet standard.

19 Q. And when you connect two computers together
20 using an ethernet cable, they would each have their own
21 IP address; right?

22 A. Again, so you're not just connecting them
23 together via ethernet cable; now you are also
24 apparently -- right, just by connecting two computers,
25 they don't get an IP address; right?

1 So you need multiple layers of software on top
2 that would, you know, give you an IP address and
3 negotiate lots of different things. So it's not just a
4 cable that you connect and, bingo, you have a network.

5 Q. Let me then rephrase the question.

6 Would you agree that it is possible to
7 physically connect two computers using an ethernet cable
8 and configure them to establish a TCP/IP connection
9 between those two computers?

10 A. With, you know -- there's a lot of things that
11 you need to do before this happens, but yes, you could
12 assign IP addresses and connect them in such a way that
13 you have a network between two computers this way.

14 Q. So in your view, you can have a network that
15 consists solely of two computers connected to each other
16 via an ethernet cable?

17 A. That's -- yes.

18 Q. And in your view, if you connect two computers
19 with each other via an ethernet cable and configured
20 them to communicate via TCP/IP, you would have a fabric;
21 right?

22 A. Well, it would be a network. And the network
23 fabric in this case is just these two boxes with the
24 cable.

25 Q. Have you also heard the phrase "fabric" in the

1 context of distributed computing?

2 A. Can you -- can you explain more -- what context
3 you are referring to?

4 Q. Do you have an understanding of a field called
5 distributed computing?

6 A. A little bit.

7 Q. What is your understanding of distributed
8 computing?

9 A. So distributed computing is when you have
10 computations occurring at multiple different places, and
11 typically, there are parts of computations happening in
12 different places.

13 Q. And have you ever heard the phrase "fabric"
14 used in connection with what you just described as
15 distributed computing?

16 A. So I believe the word "fabric" is -- is used in
17 lots of places probably; right? So -- so, you know,
18 there's only so many words you can use for physical
19 infrastructure that is used in -- for some purpose;
20 right? So you use subscript of fabric or -- but we're
21 talking about fabric in the terms -- in the context of
22 networking here; right? So the -- the context of, you
23 know, the fabric here was qualified; right? So it was
24 clear that we're talking about fabric in the context of
25 networking infrastructure.

1 Q. Well, I'm asking: Do you have an understanding
2 of the term "fabric" in the context of distributed
3 computing?

4 A. I would not want to answer that under oath
5 without doing some additional research, you know, to
6 make sure that my understanding is totally consistent
7 with -- yeah.

8 Q. Well, I mean, sitting here today, do you have
9 any understanding of what the word "fabric" means in the
10 context of distributed computing?

11 A. As I said before, the term "fabric" is very
12 often used to describe -- in many different fields to
13 describe just physical -- the physical infrastructure
14 that something is built out of.

15 Q. Now, have you reviewed Fortinet's Patent Owner
16 preliminary response submitted in this proceeding?

17 A. I have reviewed it.

18 Q. And have you reviewed the declaration submitted
19 by Dr. Black in connection with this proceeding?

20 A. I have.

21 Q. And have you reviewed the definition of fabric
22 from Newton's Telecom Dictionary that was submitted by
23 Fortinet in this proceeding?

24 A. I have.

25 Q. And have you reviewed the institution decision

1 issued by the patent office in this proceeding?

2 A. I have.

3 Q. Let me start over -- let me actually just
4 backtrack. Before I switch -- I want to revisit
5 something we discussed.

6 So you agreed, right, that a network could
7 consist of just two computers; right?

8 A. A very simple -- yeah, two -- a very simple
9 network, two computers connected. That's a network.

10 Q. And those two computers could be connected
11 wirelessly; right?

12 A. They could.

13 Q. If the two computers are connected wirelessly
14 and the first computer only has a transmitter for
15 sending data and the second computer only has a receiver
16 for receiving data, would you still consider that a
17 computer network?

18 A. It's still two computers networked together.

19 Q. Have you ever used a walkie-talkie?

20 A. When I was a kid, probably, yes.

21 Q. Would you consider a walkie-talkie a type of
22 computer?

23 MR. KLEIN: Object to scope.

24 THE WITNESS: Yeah -- so it's an analog device.

25 ///

1 BY MR. ZIVOJNOVIC:

2 Q. Let me move on to something else. So I would
3 now like to mark -- to not interfere with the exhibit
4 numbers that have been marked in this IPR and submitted
5 by the parties, I would like to enter as Exhibit A a
6 copy of the institution decision issued by the patent
7 office in this proceeding.

8 (Exhibit A marked for
9 identification.)

10 BY MR. ZIVOJNOVIC:

11 Q. Please let me know when you've had a chance to
12 download and review this document.

13 A. Okay. Yes, sir.

14 Q. If you could please go to page 3 -- let me
15 start over again.

16 Do you recognize Exhibit A?

17 A. Yes.

18 Q. Exhibit A is the institution decision in this
19 proceeding; right?

20 A. It appears to be, yes.

21 Q. And you've previously reviewed a copy of
22 Exhibit A; right?

23 A. Yes.

24 Q. If you could please go to page 3 of Exhibit A.

25 A. Yes.

1 Q. On page 3, do you see where the patent office
2 wrote, "The '825 patent describes methods of performing
3 security operations on network traffic passing through a
4 cooperative security fabric, CSF, of network security
5 appliances that coordinate their security operations to
6 avoid redundant security operations"?

7 A. Is that a question?

8 Q. Do you see that text written there?

9 A. I see that text written there.

10 Q. Do you agree with the patent office's statement
11 that, "The '825 patent describes methods of performing
12 security operations on network traffic passing through a
13 cooperative security fabric, CSF, of network security
14 appliances that coordinate their security operations to
15 avoid redundant security operations"?

16 A. Yes.

17 Q. And if you could scroll now down to page 4 of
18 Exhibit A.

19 And do you see the patent office reproduced an
20 image of Figure 2 from the '825 patent?

21 A. I see that.

22 Q. And below that, the patent office wrote,
23 "Figure 2 shows a topology 200 of a cooperative security
24 fabric that consists of the network security appliances
25 of Figure 1."

1 Do you see that?

2 A. I see that.

3 Q. Do you agree with the patent office that
4 "Figure 2 shows a topology 200 of a cooperative security
5 fabric that consists of the network security appliances
6 of Figure 1"?

7 A. I believe they're citing from the patent
8 itself, yes.

9 Q. And then if you go on to page 5, do you see
10 where it says, "Root node 220 corresponds to root
11 network security appliance 121 in Figure 1 and acts in a
12 wide area network, WAN, role that connects a private
13 network to other networks or the Internet."

14 Do you see that?

15 A. I see that.

16 Q. So if we look at Figure 2, traffic from outside
17 of an -- of the network arrives at Root 220; right?

18 A. It appears that that's what the figure is
19 trying to explain, yes.

20 Q. And then the cooperative security fabric
21 processes the traffic that's arrived at Root 2020 [sic];
22 right?

23 MR. KLEIN: Object to form and scope.

24 THE WITNESS: I'm not sure that -- you're
25 saying what? So...

1 BY MR. ZIVOJNOVIC:

2 Q. Well, Figure 2 depicts a cooperative security
3 fabric; right?

4 MR. KLEIN: Object to form.

5 THE WITNESS: So which picture -- can you
6 repeat your question, please?

7 BY MR. ZIVOJNOVIC:

8 Q. Yes. Figure 2 depicts a cooperative security
9 fabric; right?

10 A. Figure 2 shows a topology of a cooperative
11 security fabric.

12 Q. What's the difference in your view between a --
13 let me start over.

14 Is there a difference in your view between a
15 topology of a cooperative security fabric versus a
16 cooperate security fabric itself?

17 A. Well, the fabric -- the cooperative security
18 fabric appears to be, again, the physical
19 infrastructure; right? And -- and in this picture,
20 we're depicting already a -- you know, the -- a slight
21 abstraction of who connects to whom here.

22 Q. Well, it says here, "Figure 2 shows a
23 topology"; right?

24 A. Yes.

25 Q. And do you agree that Figure 2 shows a

1 topology?

2 A. Well, the patent states that Picture 2 shows a
3 topology, so I take that as -- that this is an example
4 given in the specification, yes.

5 Q. And in your view, fabric means -- let me start
6 over.

7 In your view, the word "fabric" refers to a
8 network topology, does it not?

9 MR. KLEIN: Object to form.

10 THE WITNESS: So fabric refers to the actual
11 physical infrastructure; right? So the whole point
12 about the fabric is that it's the physical thing that
13 does things.

14 BY MR. ZIVOJNOVIC:

15 Q. So is it your view, then, that the fabric is
16 not itself the topology?

17 A. The fabric expresses the topology in the real
18 world. Right? The fabric is the cables, the boxes, how
19 they're connected together, and it physically realizes a
20 topology. It expresses the topology in the real world.

21 Q. So does Figure 2 in your view depict a
22 cooperative security fabric?

23 MR. KLEIN: Object to form. Asked and
24 answered.

25 THE WITNESS: The patent specification states

1 that it does.

2 BY MR. ZIVOJNOVIC:

3 Q. Okay. And so in the '825 patent, the
4 cooperative security fabric -- I'm going to move on a
5 little bit here.

6 And so in Figure 2, we talked -- incoming
7 traffic arrives at Root 220; right?

8 A. That is what -- what it says, yes. So it says
9 Root 220 is -- corresponds to a root network appliance
10 and acts in a wide area network role that connects a
11 private network to other networks or the Internet.

12 Q. And then the incoming traffic is then processed
13 by the Leaf and Branch nodes in Figure 2; right?

14 A. I mean, so -- depending on where traffic is
15 going; right? So you're talking about incoming
16 traffic -- traffic from where to where?

17 Q. Well, I'm -- so I'm talking about traffic
18 arrives at Root 220; right?

19 A. So you're talking specifically about some
20 traffic that arrives at 220 and goes where?

21 Q. Let me start over.

22 Now, we established that Root node 220 connects
23 a private network to other networks or the Internet;
24 right?

25 MR. KLEIN: Object to form.

1 THE WITNESS: That's what it says there.

2 BY MR. ZIVOJNOVIC:

3 Q. So when traffic arrives from other networks or
4 the Internet and it's destined for the private network,
5 that traffic is processed by the Branch and Leaf nodes
6 shown in Figure 2; right?

7 A. It depends on where the traffic is going;
8 right? So this is a specific network that was designed
9 by a network architect. And so, I mean, you could have
10 traffic that is supposed to only go to 220; right?

11 Are you talking about -- where is the
12 destination of this traffic? When we talk -- when we
13 talk about traffic, we need the source, we need the
14 destination.

15 Q. Let me now -- let me mark as Exhibit 1002 a
16 copy of your declaration in this IPR proceeding.

17 (Exhibit Number 1002 marked for
18 identification.)

19 MR. ZIVOJNOVIC: It's a big file, so it will
20 take some time to process.

21 THE WITNESS: Yeah, I already have it, so...

22 BY MR. ZIVOJNOVIC:

23 Q. For record purposes, I'm still uploading; and
24 when it pops up, if you would not mind just downloading
25 it and confirming that it is indeed a copy of your

1 declaration.

2 A. Sure. Okay. Yes. Yes, sir.

3 Q. So do you recognize Exhibit 1002 as a copy of
4 your declaration?

5 A. I do.

6 Q. And if you could please go to paragraph 50 in
7 your declaration.

8 A. Yes.

9 Q. Now, at the top of paragraph 50, you write,
10 "Figure 2, below, depicts a topology of the network
11 appliances shown in Figure 1"; right?

12 A. I write that.

13 Q. And then at the bottom of that paragraph, you
14 write, "The '825 patent describes the CSF simply as the
15 result of appliances coordinating security operations
16 performed on the network traffic passing through them";
17 right?

18 A. I'm saying that in the context of the previous
19 sentence where I'm saying that "the '825 patent does not
20 define the term CSF or give it a reference numeral,"
21 yes. That's what I wrote.

22 Q. So you would agree, then, that, at a minimum, a
23 CSF must coordinate security operations performed on
24 network traffic passing through appliances?

25 A. I'm not sure about your -- your use of the

1 word -- term "must." So we're trying to use the plain,
2 ordinary meaning of this compound term, right, so we
3 have -- we know what a fabric is. We know what security
4 is. We know what cooperative is. And so the CSF has
5 the -- is apparently -- has the objective of
6 coordinating security operations on the network traffic
7 passing through them.

8 Q. Well, you applied an understanding of CSF when
9 you analyzed the prior art; right?

10 A. Yes.

11 Q. And under your understanding of CSF, do you
12 agree that it requires coordinating security operations
13 performed on network traffic passing through appliances?

14 MR. KLEIN: Object to form.

15 THE WITNESS: So the objective is that you
16 have, you know, multiple things in the -- in the fabric
17 that cooperate for the purpose of security. Right?
18 That's the -- that's the plain, ordinary meaning. So --
19 right? So I'm not sure I can think of something right
20 now, but one of the ways that you can have parts of a
21 fabric cooperating for the purpose of security is having
22 appliances coordinate security operations.

23 BY MR. ZIVOJNOVIC:

24 Q. Now, I want to drill down a bit more on the
25 network traffic at issue here. And you brought up the

1 point that we need to define the source and destination
2 of network traffic; right?

3 A. I brought that up in a specific -- because you
4 asked me a specific question that could not be answered
5 without naming what is the source and what is the
6 destination.

7 Q. Well, in the context of the '825 patent, the
8 source of the traffic or destination is the Internet or
9 other network outside of the private network; right?

10 MR. KLEIN: Object to form.

11 THE WITNESS: I -- I don't think you're
12 talking -- you're saying that all traffic in the '825
13 patent, the source is the -- outside the Internet -- the
14 outside?

15 BY MR. ZIVOJNOVIC:

16 Q. I said either the source or the destination in
17 the context of a coordinated security operation is the
18 Internet or other out- -- external network; right?

19 A. I'm not sure where you get that from. Right?
20 So -- so we have a network here, and the network is just
21 described as having a coordinate -- sorry, what was the
22 word? I'm getting -- a cooperative security fabric.
23 And, you know, the patent describes a fabric, and some
24 of the prior art that I'm citing also, you know,
25 describes a general network.

1 And then we have claims, and the claims are
2 really only interested in specific streams of packets
3 traveling from one source to one destination. So that's
4 a -- that's -- without further specifying where the
5 source or destination is. So, you know -- so I don't
6 think, you know -- what was your question again? Can
7 you repeat this?

8 Q. Let me move on to a different topic. If you
9 could please go back to Exhibit A, the copy of the
10 institution decision.

11 A. Okay.

12 Q. And this time if you could please go to page 9.

13 A. Yes.

14 Q. And do you see where the patent office wrote,
15 "At this stage of the proceeding, based on the current
16 record, we interpret 'fabric' as 'a network topology
17 such as the physical structure of a switch or network.'
18 This is consistent with an ordinary, customary meaning."

19 Do you see that?

20 A. I see that.

21 Q. And then do you see that the patent office then
22 cites Newton's Telecom Dictionary in that paragraph?

23 Do you see that?

24 A. So that's Exhibit 2003? Is that what you're --
25 is that the dictionary?

1 Q. Well, let me ask you.

2 Do you recognize Exhibit 2003 as Newton's
3 Telecom Dictionary?

4 A. I -- I just want to make sure. So let me -- I
5 have it -- I have the exhibits here. I can look at it
6 and make sure that --

7 Q. Yes, please do.

8 A. Okay. Yes, that is the dictionary. Correct.

9 Q. Okay. So here, the patent office is citing the
10 Newton's Telecom Dictionary for the ordinary and
11 customary meaning of fabric; right?

12 A. Yes.

13 Q. Do you agree that the definition in Newton's
14 Telecom Dictionary reflects the ordinary and customary
15 meaning of fabric?

16 A. It's consistent with -- yes.

17 Q. Let me now mark as Exhibit 1001 a copy of the
18 '825 patent.

19 (Exhibit Number 1001 marked for
20 identification.)

21 MR. ZIVOJNOVIC: By the way, actually -- we've
22 been going not quite an hour, but we've been close to an
23 hour. Since we're moving on to a different exhibit, now
24 would be a convenient time to take a break. But I'm
25 happy to also keep going if you prefer. I just want to

1 flag --

2 THE WITNESS: I'll take a five-minute break,
3 please.

4 MR. ZIVOJNOVIC: All right. Let's do it.

5 THE WITNESS: Okay.

6 MR. ZIVOJNOVIC: Let's go off record, please.
7 (Off the record.)

8 BY MR. ZIVOJNOVIC:

9 Q. So, Dr. Franz, have you had a chance to
10 download and review Exhibit 1001?

11 A. Yes.

12 Q. Exhibit 1001 is a copy of the '825 patent;
13 right?

14 A. Yes.

15 Q. I want to start by looking at Figure 1, if you
16 could please go there.

17 A. Yes.

18 Q. So if we look at Figure 1 on the right, do you
19 see appliances 121, 130, and then 140?

20 MR. KLEIN: Object to form.

21 THE WITNESS: So I see -- I see there are boxes
22 labeled 121, 130, and what was the third one?

23 BY MR. ZIVOJNOVIC:

24 Q. 140.

25 A. And 140 with a, b, and c.

1 Q. Do you agree that Figure 1 there depicts three
2 layers of network security appliances?

3 A. So Figure 1 depicts an -- well, what does it
4 exactly say? It depicts a specific network
5 architecture; right? An exemplary network architecture
6 in accordance with one embodiment of the present
7 invention. That's what it depicts.

8 Q. And do you agree that the network architecture
9 in Figure 1 shows three layers of network security
10 appliances?

11 A. It shows -- well, it shows a hierarchical
12 network architecture in which you have a tree-shaped
13 architecture in which you have three different layers of
14 the network.

15 Q. And network security appliances 140a through
16 140d are at the perimeters of subnets 141a through 141d;
17 right?

18 A. Right. So -- so the patent calls it -- yes.
19 The patent says, "Each of the subnets, 141a to 141d, may
20 connect to a subnet network security appliance 140a to
21 140d that separates a subnet from external computing
22 environment." I'm reading from the patent
23 specification.

24 Q. And would you agree that these subnets 141a
25 through 141d comprise user computers?

1 A. I don't know what they comprise. Does it say
2 in the specification? I did not remember the whole
3 specification. I mean, this is a -- an example
4 architecture that the patent specification is talking
5 about.

6 Does it say so? I'm sorry. I do not -- have
7 not memorized the whole specification.

8 Q. Well, I'm asking, do you have an understanding
9 of whether subnets 141a through 141d include end user
10 computers?

11 A. I mean, depends on what specific -- the
12 architect wanted here, but for the -- you know, it would
13 make sense that such an architecture could be used in
14 which the subnets in a -- in a private corporate network
15 would be -- would include end user computers.

16 Q. And if you could please now go to Column 5,
17 starting at line 32. Let me know when you're there.

18 A. Okay.

19 Q. So here in the '825 patent it says, "In the
20 present example, downstream network traffic that is
21 transmitted from the Internet 110 to a subnet 141 goes
22 through three network security appliances, i.e., a root,
23 a middle, and a subnet network security appliance, while
24 upstream traffic that is transmitted from subnet 141 to
25 the Internet goes through a subnet, a middle, and a root

1 network security appliance."

2 Do you see that?

3 A. I see that.

4 Q. And then the next sentence says, "Each network
5 security appliance on a network path has the ability to
6 execute the same security operations based its local
7 security policies [sic]."

8 Do you see that?

9 A. I see that.

10 Q. And then if you go further down, starting at
11 line 43, "In embodiments of the present invention, the
12 root, middle, and subnet network security appliances
13 form a cooperative security fabric that coordinates
14 operations among members and avoids redundant operations
15 even when local policies define the same operations."

16 Do you see that?

17 A. I see that.

18 Q. So in embodiments of the present invention, the
19 root, middle, and subnet network security appliances of
20 Figure 1 form a cooperative security fabric.

21 Do you agree with that?

22 A. That's what the patent specification says.

23 Q. And in Figure 1, the traffic that is being
24 processed by this cooperative security fabric is either
25 downstream traffic -- network traffic from the Internet

1 to a subnet or upstream network traffic from a subnet to
2 the Internet; right?

3 A. I don't think that's all the traffic. Right?
4 So in networks, there's probably also traffic going from
5 one subnet to another subnet and -- you know, I mean,
6 that's what networking is about; right? So, you know --
7 but there's probably some traffic from the Internet to a
8 subnet. I don't know what's -- you know, but the whole
9 point of this network architecture appears to be that
10 things are connected.

11 Q. Well, if we're looking at the '825 patent --
12 actual description of Figure 1, though, it's
13 specifically talking about downstream network traffic
14 from the Internet to subnets and upstream network
15 traffic from subnets to the Internet; right?

16 A. So it gives two examples. So this is an
17 example, and it gives two examples of traffic. One
18 traffic -- one example of traffic is traffic that starts
19 on the outside Internet and goes down to a subnet, and
20 it also gives an example of an -- it calls that
21 downstream. And it has a second example of a -- of
22 traffic that starts at a subnet and goes out to the
23 Internet.

24 Q. I believe you testified that, in theory, you
25 could also process traffic between two different

1 subnets; right?

2 A. I don't know. I mean, it -- we are -- we don't
3 have any more information here. We have examples of
4 traffic that the network designer wanted to be there.
5 Right? So it very much depends on how you design your
6 network.

7 Q. So fair to say, then, that the '825 patent does
8 not include examples of network security appliances
9 processing traffic between two subnets?

10 A. The specification example that you're citing
11 there does not -- mentions exemplarily traffic from the
12 Internet to a subnet and from a subnet to the Internet.

13 Q. And you're not aware of other examples in the
14 '825 patent that talks about performing security
15 operations on traffic between two subnets, are you?

16 A. In the specification, there's no example like
17 that.

18 Q. If you could please now go to Figure 2 of the
19 '825 patent.

20 A. Yes.

21 Q. And I'm just going to -- sorry, I'm just
22 rotating the figure for my own sanity.

23 A. Yeah, I should probably do that myself. One
24 second. Okay. Here we go.

25 Q. So what the '825 patent describes as downstream

1 traffic arrives at Root 220; right?

2 A. It appears so.

3 Q. And at that point, traffic that is received at
4 Root 220 from the Internet, if it's not destined for the
5 root itself, would be forwarded on either Branch 230a,
6 Leaf 250 or Branch 230b; right?

7 A. Well, if the destination is along that route.
8 Perhaps you could tell me what the destination of the
9 traffic is.

10 Q. I guess let me establish this. What's shown
11 in -- do you have -- let me start over.

12 Do you understand what is shown as Leaf 240a
13 through d corresponds to security appliances guarding
14 individual subnets?

15 A. Yeah, I believe that these Leaf 240a through d
16 correspond to 140a to d in Figure 1.

17 Q. So if traffic is received at Root 220 and it is
18 destined for subnet 141a, it would traverse Root 220,
19 Branch 230a, and Leaf 240a; right?

20 A. So seeing that there are no other routes, that
21 it would seem that the route from the outside world to a
22 Leaf 240a would go to 220, 230a, and then 240a.

23 Q. And traffic destined for subnet 141d would
24 traverse Root 220, Branch 230b, and Leaf 240d; right?

25 A. So traffic from the outside world to 240d

1 would, in this topology, have to pass through 220 and
2 then 230b and then 240d.

3 Q. So would you agree that at each level -- let me
4 start over.

5 Do you agree that in Figure 2, depending on
6 destination, traffic from the Internet could traverse
7 different combinations of branch and leaf network
8 security appliances?

9 MR. KLEIN: Object to form.

10 THE WITNESS: So this is -- this is a
11 tree-shaped architecture where the whole purpose is
12 that, you know, you find the stream of the traffic down
13 the tree in this case.

14 BY MR. ZIVOJNOVIC:

15 Q. So you would agree that depending on traffic
16 destination, different branches and leaves would be
17 responsible for processing the traffic?

18 A. The whole Internet works like that; right?
19 Depending on any combination of source and destination,
20 you pass through different paths. So the way that this
21 network is designed is that traffic to, you know,
22 different leaves passes along different routes.

23 Q. But a set of network security appliances
24 responsible for processing particular traffic would
25 depend on the traffic's destination; right?

1 A. So the set of nodes on the network that are
2 touched by a packet going from source to destination
3 depends on the destination.

4 Q. And so I just want to make sure in the context
5 of the '825 patent specifically, that means that
6 depending on destination, a different set of network
7 security appliances may process the traffic; right?

8 A. So the network security appliances that are
9 involved in the path of -- from the outside world to a
10 leaf differs depending on what the target is.

11 Q. And then do you see Leaf 250 that is connected
12 directly to Root 220?

13 A. I see that.

14 Q. An endpoint connected -- let me start over.

15 Internet traffic destined for an endpoint
16 connected to Leaf 240a would go through processing by
17 three different network security appliances; right?

18 A. So in this specific topology, there are three
19 hops to go to a Leaf 240 and only two to go to a
20 Leaf 250.

21 Q. So then maybe I can just jump to what I
22 wanted -- you know, skip -- I think you're getting a
23 little ahead of me, so let me, I guess, ask the next
24 question, which is:

25 So would you agree that in the context of the

1 '825 patent, the number of network security appliances
2 responsible for processing incoming Internet traffic may
3 depend on the destination of that traffic?

4 A. So in this example, clearly, the number of, in
5 this case, routers, you know, these boxes -- yeah,
6 there's -- there are different numbers of these
7 appliances in the path from an outside source to a
8 destination, depending on which part of the tree you're
9 in.

10 Q. I would now like to mark as Exhibit 104 [sic] a
11 copy of the Chandra patent application.

12 (Exhibit Number 1004 marked for
13 identification.)

14 BY MR. ZIVOJNOVIC:

15 Q. Please let me know when you've had a chance to
16 download and review this document.

17 A. Okay. I see that.

18 Q. And you recognize Exhibit 1004 as a copy of
19 Chandra; right?

20 A. I do.

21 Q. Now, Figure 1 in Chandra illustrates a network
22 environment 100 for implementing an embodiment of the
23 present invention. And I'm reading that from
24 paragraph 21.

25 Do you see that?

1 A. I see that.

2 Q. So in Chandra's -- and if we -- let me start
3 over. And then if we keep on reading two sentences
4 below that, "Network 102 can be a collection of
5 individual networks, interconnected with each other and
6 functioning as a single large network."

7 Do you see that?

8 A. Where do you write this -- where is this?

9 Q. This is the -- this is still in paragraph 21,
10 third sentence.

11 A. Okay. Yes.

12 Q. So the network environment of Chandra's
13 Figure 1 functions as a single large network.

14 Agreed?

15 A. Can you ask the question again, please?

16 Q. The network environment of Chandra's Figure 1
17 functions as a single large network.

18 Agreed?

19 MR. KLEIN: Object to form.

20 THE WITNESS: So, I mean, we have a network in
21 the middle called 102; right? So what are you --
22 everything is a single large network, right, depending
23 on -- I mean, where -- where do you -- where do you draw
24 boundaries?

25 What exactly is your question?

1 BY MR. ZIVOJNOVIC:

2 Q. Well, Chandra says that its network 102
3 functions as a single large network, does it not?

4 A. So network 102 -- 102 is -- functions as a
5 single large network. Yes. That's what Chandra says.

6 Q. And then -- let me start over.

7 And then if you see -- Chandra also has
8 Figure 2 -- if you could go there, please.

9 A. Yes.

10 Q. All right. And Chandra's Figure 2, again, also
11 references network 102; right?

12 A. Yes.

13 Q. And in Chandra's Figure 2, both the
14 transmitting end and the receiving end are connected to
15 the same network 102; right?

16 A. I see that.

17 Q. And if you could please go to Chandra's
18 Figure 8. Let me know when you're there.

19 A. I'm there.

20 Q. And do you see that in Chandra's
21 Figure 2 [sic], both the transmitting end and the
22 receiving end are also connected to the same network
23 102?

24 A. You mean -- you said in Figure --

25 Q. Let me -- if I said Figure 2, let me re-ask the

1 question. I was intending to ask about Figure 8.

2 Do you see that in Chandra's Figure 8, both the
3 transmitting end and the receiving end are connected to
4 the same network 102?

5 A. They're inside the box that says network 102.

6 Q. Now, Chandra uses the term "VPN"; right?

7 A. It does.

8 Q. And "VPN" stands for virtual private network;
9 right?

10 A. That is my understanding.

11 Q. What is a virtual private network?

12 A. So a virtual private network is a network in
13 which some of the connections are transiting the public
14 Internet, but they are realized as a secure tunnel so
15 that no party that observes the traffic or that handles
16 the traffic across the tunnel can see what's inside the
17 tunnel or modify it.

18 Well, they -- it's -- they use cryptographic
19 technology. So it's trying to establish a private
20 tunnel that you can then route the traffic via, you
21 know, potentially dangerous infrastructure, but it acts,
22 for our purposes, as if it were your own private
23 connection.

24 Q. And is it fair to say that one of the purposes
25 of VPN technology is that from the perspective of the

1 two endpoints, even though they are remote from each
2 other, they appear to be connected to the same virtual
3 private network?

4 A. Yeah. So the two endpoints appear to be
5 connected.

6 Q. I want to take a closer look at Chandra's
7 Figure 2, if you could please go there.

8 A. I'm there.

9 Q. So Chandra's Figure 2 shows transmission of
10 network traffic from a transmitting end to a receiving
11 end that are both on the same network 102; right?

12 A. So -- yeah, it focuses on traffic that is going
13 from the 206 to 212 using -- using 102.

14 Q. Now, in your invalidity mapping for Chandra, am
15 I correct that you are mapping the claimed second
16 network security appliance to transmitting customer edge
17 208?

18 A. I believe I am, but if you would like -- if I
19 could have a quick look at my declaration. I believe
20 that is correct.

21 Q. And in your invalidity mapping for Chandra, am
22 I correct that you're mapping the claim first network
23 security appliance to receiving customer edge 214?

24 A. The receiving customer edge is the first
25 network security appliance, yes.

1 Q. Can Chandra's receiving customer edge 214 also
2 receive traffic from the Internet?

3 MR. KLEIN: Object to scope.

4 THE WITNESS: I'm -- so Chandra explains a
5 particular path that traffic takes, you know, when it
6 transits from a transmitting end to a receiving end;
7 right? So Chandra just tells us very specifically what
8 happens to a sequence of packets that are going from 206
9 to 212 and the path that they take. Right?

10 It doesn't tell us anything about the rest of
11 the network topology because that is not essential for
12 this particular method that Chandra is telling us about
13 of how you avoid redundant operations by having these
14 two ends communicate and cooperate with each other.

15 BY MR. ZIVOJNOVIC:

16 Q. And Chandra also does not disclose forwarding
17 traffic that was received by receiving customer edge 214
18 from transmitting customer edge 208 to any other third
19 customer edge, does it?

20 A. Chandra tells us, you know, very specifically
21 about a method of avoiding redundant operations in a
22 setup where you have a packet traveling from 206 to 212,
23 and you're using the headers of that packet to
24 communicate to the receiving customer edge about any
25 rules you may have already -- any security operations

1 you may already have applied at 208. We don't know what
2 else is happening in that system.

3 Q. Let me maybe ask it this way.

4 In your invalidity mapping for Chandra, you are
5 relying on traffic being processed by both transmitting
6 customer edge 208 and receiving customer edge 214;
7 correct?

8 A. I don't know what you're meaning by
9 "processed." So the transmitting customer edge and the
10 receiving customer edge are providing the security
11 functionality. And we are looking at a sequence of
12 packets that is traveling from 206 to 212.

13 Q. All right. So the particular network traffic
14 that you're pointing to is from 206 to 212; right?

15 A. That is the example given in Chandra.

16 Q. And in the example from Chandra that you're
17 relying on, the traffic from 206 to 212 would be
18 processed by two customer edges, transmitting customer
19 edge 208 and receiving customer edge 214; right?

20 A. These are the parts that are doing the physical
21 transmission, but they're not the parts that are doing
22 the -- the customer edge is the component that has the
23 security functionality.

24 Q. But you did not identify in Chandra any
25 instance where network traffic traverses three customer

1 edges that have security functionality; correct?

2 A. I actually provided an example where I'm
3 cascading Chandra, right, for one of the dependent
4 claims.

5 Q. We'll get to that. Let's go to paragraph 96 of
6 your declaration first, please.

7 A. Okay.

8 Q. Let me know when you're there.

9 A. Okay.

10 Q. And do you see in the second sentence where you
11 write, "If the data packet did not have a recognized
12 label, e.g., the traffic originated from the Internet,
13 the receiving CE identified the packet as non-secure and
14 performed a third set of actions on the packet."

15 Do you see that?

16 A. I see I write that.

17 Q. And I jumped to the last clause of the final
18 sentence. Do you see where you wrote, "An unregistered
19 CE label or absence of the CE label indicated that the
20 data packet was not transmitted from the transmitting
21 CE"?

22 Do you see that?

23 A. I see that.

24 Q. So do you agree that in Chandra, in the case of
25 traffic originating from the Internet that is received

1 by a receiving CE, that traffic was not transmitted from
2 a transmitting CE?

3 A. So we're talking about a specific pair of
4 transmitting and receiving CEs that have previously
5 communicated to establish their -- you know, their
6 shared secret handshake; right? So first, they
7 authenticate, then they trade labels.

8 So it is not any CE; it is the specific CE that
9 is known and authenticated in the setup of this -- of
10 this connection. So I can identify traffic that comes
11 from the specific transmitting CE that I have previously
12 established a relationship with.

13 Q. Does Chandra disclose examples of network
14 traffic that is not transmitted from a transmitting CE?

15 A. I do not believe it establishes an example, but
16 it -- I'm quoting here from Chandra, right, so -- so
17 what is 47 to 53 -- right.

18 So Chandra talks about it is possible that the
19 data packet has not been tagged with a CE label or the
20 tagged CE label is not recognizable by either receiving
21 CE; and, in this case, Chandra teaches to apply a third
22 set of actions on the data packet in, you know -- so
23 Chandra apparently contemplates traffic that doesn't --
24 well, that wasn't labeled by the corresponding CE.

25 Q. My question is simpler. Let me start over.

1 Does Chandra disclose a receiving CE receiving
2 traffic that originated from the Internet?

3 A. Chandra discloses traffic that is not labeled,
4 and we don't know why.

5 Q. So your position is that Chandra does not
6 expressly disclose one way or the other whether a
7 receiving CE can receive traffic originating from the
8 Internet.

9 A. So in paragraph 53, Chandra says, you know,
10 "Moreover, when receiving CE 214 receives a data packet
11 from the Internet, it performs actions corresponding to
12 rules regarding such data packet" to "ensure that the
13 data packet is secure and safe." Right?

14 And -- and so the receiving CE 214 does receive
15 traffic from the Internet, and precisely that the
16 traffic -- that -- if it has that -- the flag in it,
17 then it came from the transmitting customer edge; that
18 is when it doesn't have to do the redundant operations.

19 Q. So your position is that Chandra does disclose
20 that receiving CE 214 can receive traffic that
21 originated from the Internet?

22 A. The specification talks about -- you know,
23 mentions in paragraph 53 that I -- that I mentioned, it
24 says -- it talks about "when receiving CE 214 receives a
25 data packet from the Internet, it performs actions

1 corresponding to rules regarding such data packet," and
2 then it talks about how, by applying this coordination,
3 this cooperation between these two things, by traffic
4 that first went through the transmitting CE, you don't
5 have to do -- you don't have to do these operations that
6 have already been performed.

7 Q. And that's because in that case, it has already
8 gone through the transmitting CE; right?

9 A. Because in that case it has gone through the
10 previous consumer edge that did the security functions.

11 Q. So -- but in the case where Chandra receives
12 traffic from the Internet, there's only a single CE 214
13 that performs the security functions; right?

14 A. We don't know that. We don't know where else
15 it's gone through. We're talking very specifically in
16 this patent about one packet that happened to come
17 through the 208 and then goes through the 214. And
18 because it went to the 208; and 208, which is previously
19 known to 214, included a flag in the packet saying that
20 I have already done this, this, and this; and I'm doing
21 that by communicating a special flag that tells me I've
22 done these operations; then 214 is confident that 208
23 did these operations, and then it can decide whether to
24 skip these operations, do them again, partially do them
25 again, or whatever, depending on its local policies.

1 So Chandra tells us this is how you avoid the
2 redundant operations. It doesn't tell us anything else
3 about anything else that might also happen in this
4 network. Or at least, you know, it tells us other
5 things, but the relevant things to the claims are only
6 what happens to the one packet that passes through
7 multiple of these cooperating security fabric devices,
8 appliances; and how does their collaboration,
9 cooperation allow me to reduce redundancy in the
10 security work that I'm doing.

11 Q. Is it your position, then, that Chandra does
12 not explicitly provide an example where traffic is
13 processed only by a single receiving CE?

14 A. Well, it -- the paragraph I already read to you
15 kind of implies that, doesn't it?

16 Q. Well, sir, my question is -- it's -- I'm just
17 asking you: When you read this paragraph and when this
18 traffic received from the Internet -- does that mean --
19 let me start over.

20 I'm asking for your understanding of Chandra,
21 and specifically, is it -- whether or not it's your
22 understanding that when traffic originates from the
23 Internet in Chandra, is it only a single receiving
24 CE 214 that performs the security functions, or is it
25 your position that there still is a second

1 transmitting CE, even in that scenario, that also
2 performs the security function?

3 MR. KLEIN: Object to form.

4 THE WITNESS: First of all, the transmitting CE
5 does not perform these functions; right? It's --
6 it's -- yeah. Okay. So the transmitting -- well, so
7 Chandra is concerned, you know -- it's not telling us
8 all about networking. Its concerned about the specific
9 technique of avoiding redundant work.

10 And so all it's telling us is that I have a
11 receiving customer edge, I get traffic, and if that
12 traffic is from a known party that I've previously
13 established a relationship with and I have established a
14 communication, you know, basis that tells me this flag
15 means this and this flag means this and this flag means
16 this, then I can elect to not have to do certain
17 operations because I know for sure that they have
18 already been done somewhere on my incoming path for the
19 packet.

20 That's all I'm telling -- that is being told
21 there. But the fact that it is talking about -- that
22 there is the possibility that traffic might not have
23 these flags would indicate to me and also to a person of
24 ordinary skill in the art that there are paths that --
25 on which you have not previously passed through a

1 previously established, known, other cooperating
2 security device. Right?

3 Otherwise, why do this? Why bother? Right?
4 If I know that I'm always coming through, I wouldn't
5 have to do this. This is -- this application is
6 teaching us, you know, if you can prove you came through
7 a previous device, because you have actually established
8 a relationship with that device beforehand, then you
9 don't have to do these operations again. That's all
10 it's teaching us.

11 BY MR. ZIVOJNOVIC:

12 Q. You do believe that Chandra teaches instances
13 of where traffic may be processed by just a single CE
14 component that performs security functions. Fair?

15 MR. KLEIN: Objection. Asked and answered.

16 THE WITNESS: It doesn't teach this. It
17 implies it because, you know, the whole point here is
18 that you have traffic arriving; and if the traffic has
19 the flag of the cooperating security appliance, then you
20 know it's come from there.

21 And since we have a flowchart that says if it
22 has that -- if it has that flag -- and we have a lot of
23 discussion about what are these flags. That would imply
24 that there are situations where you don't have this
25 flag. And if you don't have this flag, that would

1 indicate that there is traffic that somehow arrives at
2 the receiving customer edge without having gone through
3 the transmitting customer edge.

4 BY MR. ZIVOJNOVIC:

5 Q. If traffic arrives from outside of network 102
6 at receiving CE, it would not have gone through the
7 transmitting CE; right?

8 A. I don't know. We are not -- all we are
9 concerned about here is we're concerned about specific
10 packets that, on their way to the receiver from the
11 transmitter, went through both 808 and 814. And if they
12 went through 808, then 814 can elect to do less work.

13 And if there is any path somehow that gets to
14 814 without going through 808, then we can detect that
15 because of the missing flag, and we act accordingly.
16 That is what this patent teaches us -- or this patent
17 application.

18 MR. KLEIN: Ogi, we've been going about an
19 hour. Is now a good time for a break?

20 MR. ZIVOJNOVIC: Let me see here. Yeah, might
21 as well. Why not.

22 THE REPORTER: Okay. We're off the record.
23 (Off the record.)

24 THE REPORTER: Okay. We're on the record.

25 ///

1 BY MR. ZIVOJNOVIC:

2 Q. If you could -- you have a copy of the '825
3 patent; right?

4 A. I do. Yes.

5 Q. If you could please go to Claim 6. And let me
6 know when you're there.

7 A. One second. Okay. Yes.

8 Q. Now, Claim 6 of the '825 patent requires -- and
9 I'm going to read from the last piece of it.

10 Claim 6 requires "a next network appliance
11 participating in the CSF."

12 Do you see that?

13 A. I see that.

14 Q. So for Claim 6, we have our first network
15 security appliance, a second network security appliance,
16 and then a next network appliance; right?

17 A. Yes.

18 Q. Apologies. And if you could now go --

19 A. I think -- sorry. I think you -- you broke up
20 there. I didn't --

21 Q. Oh, I just coughed, and I said apologies.

22 A. Oh, okay. Just making sure.

23 Q. If you could please go to paragraph 123 of your
24 declaration. Let me know when you're there.

25 A. Yes.

1 Q. And so paragraph 123 addresses the limitation
2 that requires a next network appliance participating in
3 the CSF; right?

4 A. So it addresses Claim 6, yes.

5 Q. And in paragraph 123, you write, "Buruganahalli
6 disclosed network device 52 transmitted the network
7 traffic with the updated flag to network device 50,
8 which was another device participating in the CSF."

9 Do you see that?

10 A. I see that. I wrote that.

11 Q. So for the claim "next network appliance
12 participating in the CSF," is it fair to say you were
13 pointing to Buruganahalli's network device 50?

14 A. Let me -- what was your question?

15 Q. For the claim "next network appliance in the
16 CSF," are you pointing to the network device 50 from
17 Buruganahalli?

18 A. So it's whatever -- whatever cooperative
19 network device next does, you know -- next does a
20 security operation on the packet that comes out with the
21 modified metadata tag.

22 Q. Well, you -- for Claim 6, you're combining
23 Chandra with Buruganahalli; right?

24 A. Correct. So Buruganahalli tells us that we can
25 have many of these devices, and there is -- instead of

1 each of these devices adding its own header -- separate
2 header and tags, which you would then have to go and
3 dissect in sequence, you actually have a compound
4 metadata that is updated by the different devices in the
5 chain as you go along. Right?

6 So there's not exactly three. So every device
7 in Buruganahalli has, like -- well, the first one is
8 special; the last one is special; but the ones in the
9 middle, they come with a metadata tag, and the metadata
10 tag already contains some information. And you update
11 the information after you've done something, and then
12 you pass it on. That is what Buruganahalli teaches us.

13 And it also teaches us that the very first
14 device in the chain, if there is no metadata tag, can
15 add one. And I believe it also teaches us that the last
16 one can remove it. But the point is that you have the
17 devices in the middle -- they have the -- they see a
18 metadata tag, they know what's already been performed by
19 all the devices that already went through the
20 cooperating devices on the way here, and they update
21 with what the device currently processing the packet has
22 been doing.

23 Q. In paragraph 123, you're stating, though, that
24 Buruganahalli's network device 50 is another device
25 participating in the CSF; right?

1 A. So I see that I wrote that. Yes.

2 Q. Okay. So do you contend that Buruganahalli's
3 network device 50 is a next network appliance
4 participating in the CSF?

5 A. So Buruganahalli disclosed that network
6 device 52 could be configured to send network data 58 to
7 network device 50, yes.

8 Q. So I would now like to mark Exhibit 1008
9 corresponding to the Keohane prior art reference.

10 A. Okay. I have it open.

11 (Exhibit Number 1008 marked for
12 identification.)

13 BY MR. ZIVOJNOVIC:

14 Q. And if you would please go to Figure 3 in
15 Keohane.

16 A. I see that.

17 Q. So in Keohane, a data packet 306 is first
18 received by firewall 300; right?

19 A. That is the flowchart here, yes.

20 Q. And firewall 300 then forwards the data packet
21 to mail gateway 302?

22 A. The path goes through mail gateway and then to
23 the client, yes.

24 Q. And so then to wrap it up, the mail gateway
25 then forwards the data packet to client 304; correct?

1 A. That is what this picture shows, yes.

2 Q. And can you please go to paragraph 33 in
3 Keohane. Let me know when you're there.

4 A. I am there.

5 Q. And do you see in the 6th line of paragraph
6 33 -- I'm sorry, in the 5th line of paragraph 33 where
7 it says, "Data packet 306 is received by firewall 300."

8 Do you see that?

9 A. I see that.

10 Q. And then do you see in paragraph 304 [sic] at
11 the beginning where it says, "If data packet 306 is
12 determined to be from a trusted source, firewall 300
13 allows data packet 306 to be passed to mail gateway
14 302."

15 Do you see that?

16 A. Yes.

17 Q. And in your -- let me start over.

18 So fair to say that in Keohane, your disclosure
19 is that data packets -- let me start over.

20 Are data packets in Keohane always received by
21 firewall 300 initially?

22 A. So Keohane in Figure 1 shows a network in which
23 you have servers and clients, you know, communicating --
24 I believe it uses the word "with each other" or "among
25 each other" or something.

1 So there is, you know -- it's a network, and
2 packets -- who knows. Right? Who knows how the network
3 is architected. Again, the flowchart is illustrative to
4 the specific method that is described in this patent,
5 just like the illustration in Chandra is illustrative to
6 the specific method that is described, which is
7 operating on specific packets that are going from one
8 place to another and which are passing multiple elements
9 of the cooperative security fabric along the way.
10 Right?

11 So we don't know what else is happening in this
12 network. All we are -- all that we need to know for
13 understanding the invention that this lady or gentleman
14 is trying to describe to us is we have a packet, the
15 packet is passing along several elements of this
16 cooperating security apparatus, and the first element is
17 marking something using a flag so that the second
18 element doesn't need to repeat the operation.

19 That's what it's telling us. And it's doing
20 that by way of an illustration, which was Figure 3,
21 which is, you know, something happening in the larger
22 Figure 1.

23 Q. So --

24 A. I lost my -- since I go back and forth, I lost
25 my place. What paragraph were we at, please?

1 Q. So we're looking at paragraph 33 and 34.

2 A. Okay.

3 Q. But as to what Keohane explicitly describes, it
4 teaches that every data packet goes through firewall
5 300, then mail gateway 302, and then client 304, does it
6 not?

7 A. It says --

8 MR. KLEIN: Object to form.

9 THE WITNESS: -- it illustrates -- it
10 illustrates a multiple-level security system because it
11 uses that example to describe the method that is being
12 used to avoid redundant security operations.

13 BY MR. ZIVOJNOVIC:

14 Q. Does Keohane explicitly disclose an example
15 where a data packet is received by the mail server
16 without first going through the firewall?

17 A. Well, the mail gateway in 35 examines the data
18 packet to determine whether there is a signature from a
19 trusted security element present. And in this case, you
20 know, it -- so again, in this -- so in the example, the
21 firewall added one, which means the mail gateway can
22 elect not to do certain security operations.

23 And, you know, just reading this, it implies
24 that there also are situations in which there is no such
25 signature. Right? So -- but I'm describing a method to

1 avoid redundant operations. And for that, I'm just
2 giving an example how you avoid the redundant
3 operations. I don't know what else is happening in that
4 network. It doesn't matter to this -- to this specific
5 explanation.

6 Q. I'm just asking about the explicit disclosure.
7 I'm not asking about what else, in theory, could be
8 happening --

9 A. It's not theory. It's the fact that it -- that
10 Keohane describes that there needs to be a determination
11 whether or not a signature from a trusted security
12 element is present. That tells me and that would tell a
13 person of skills -- ordinary skill in the art at the
14 time that there are situations in which it's not
15 present.

16 And because of this little picture that you
17 showed me, you know, as a path that goes through that,
18 that means that there are apparently ways where you
19 could get to the mail server not going via this path.
20 Because going through this path, you would have the
21 signature.

22 Q. In your invalidity analysis, Keohane's firewall
23 is the second security network appliance; right?

24 MR. KLEIN: Object to form.

25 THE WITNESS: Let's go back. So ask your

1 question again.

2 BY MR. ZIVOJNOVIC:

3 Q. In your invalidity analysis, Keohane's firewall
4 is the second security network appliance; right?

5 MR. KLEIN: Same objection.

6 THE WITNESS: So in the -- I mean, we talked
7 about having -- well, so here, there are two devices in
8 this example, and -- yes, so the firewall is the
9 security appliance that receives the package first,
10 which in the claims of the patent, it's called a second
11 one; and the mail gateway is the cooperating network
12 appliance that can elect to suppress the redundant
13 operations based on the flag that it sees on the
14 traffic.

15 BY MR. ZIVOJNOVIC:

16 Q. So for the claimed first network security
17 appliance, you're pointing to Keohane's mail gateway;
18 right?

19 A. Sure that I'm doing that consistently, but --
20 okay. Can you re-ask your question, please?

21 Q. In your invalidity theory, the claimed first
22 network security appliance corresponds to Keohane's mail
23 gateway; right?

24 A. Can you point to a specific claim where I'm --

25 Q. Sure.

1 A. -- the specific analysis where -- where I'm --

2 Q. If you look at paragraph 160.

3 A. My paragraph 160?

4 Q. Yes. Paragraph 160 of your expert report.

5 A. Thank you. Okay. Perfect.

6 So in 162, yes, I'm pointing to the mail
7 gateway 302 being a first network security appliance.
8 And then -- and I'm saying that could be any network
9 appliance in the appliance chain.

10 Q. Can you please go to paragraph 166?

11 A. Yes.

12 Q. And in paragraph 166, you wrote, "Figure 7,
13 below, for example, depicted a process flow for
14 performing a security action in Keohane's security
15 elements, e.g., mail gateway."

16 Do you see that?

17 A. I see that.

18 Q. And then you go on to quote from Keohane
19 paragraph 35, "A trusted security element was a network
20 element such as a firewall, mail gateway, router, or
21 some other security intermediary that performed a
22 security action on a data packet."

23 Do you see that?

24 A. I see that.

25 Q. So fair to say that Keohane's Figure 7 shows

1 the operation of both Keohane's firewall and Keohane's
2 mail gateway?

3 A. Figure 7 shows how you -- how you -- is a
4 general flowchart how you would be able to examine the
5 signature headers, then identify, you know, the --
6 authenticate the -- that the -- that this header
7 actually was added by a cooperating entity in your
8 system.

9 Then it would identify what security action was
10 to be done based on what you learned about previous
11 security actions having been performed, if such a header
12 is present, if flags are present. And then if -- then
13 you do the action. And then at the end, you add the
14 signature of what you've just done so that devices
15 downstream of you in the traffic can do the same action.

16 So this is the core of how you avoid redundant
17 operations. And the whole point is that, you know, all
18 the cooperating elements of your cooperative security
19 fabric do these operations.

20 Q. So my question's simpler than that. It is
21 just: Am I correct that the teachings of Figure 7 apply
22 not just to Keohane's mail gateway, but also Keohane's
23 firewall?

24 A. Well, these teaching apply to the -- explain
25 how the cooperation works between these elements. So --

1 Q. Explain how the cooperation -- does Figure 7
2 explain how the cooperations of Keohane's firewall work?

3 MR. KLEIN: Object to form.

4 THE WITNESS: It explains how you cooperate
5 between, you know, elements that perform collaborative,
6 cooperative security functions.

7 BY MR. ZIVOJNOVIC:

8 Q. Well, Figure 7 -- let me take a look at
9 something really quick.

10 If you go to paragraph 52 of Keohane -- let me
11 know when you're there.

12 A. Yes. So it's actually just one embodiment of
13 this; right? So...

14 Q. Just let me know when you're in paragraph 52.
15 That's all I'm asking.

16 A. So 52 tells us this is an illustrative
17 embodiment.

18 Q. So you are at paragraph 52. That's all I was
19 asking.

20 A. Correct.

21 Q. Okay. Thank you. The second sentence of
22 paragraph 52 says, "The process illustrated in Figure 7
23 may be implemented in a security element or some other
24 data processing system within a network."

25 Did I read that correctly?

1 A. You did.

2 Q. Okay. If we now go back to paragraph 166 of
3 your declaration.

4 A. Yes.

5 Q. And so here you address -- let me start over.

6 In here, you write, "Figure 7, below, for
7 example, depicted a process flow for performing a
8 security action in Keohane's security elements, e.g.,
9 mail gateway"; right?

10 A. I wrote that.

11 Q. So in Figure -- and then at the last sentence,
12 you write, "At step 700, the security element, e.g.,
13 mail gateway, received a data packet."

14 Do you see that?

15 A. I see that.

16 Q. All right. Now, you wrote "e.g. mail gateway";
17 right?

18 A. I wrote that.

19 Q. "E.g." means if -- for example, could be done
20 in the mail gateway; right?

21 A. Correct.

22 Q. Is it also correct that Figure 2 -- sorry.

23 Is it also correct that Figure 7 depicts a
24 process flow for performing a security action in
25 Keohane's security element, e.g., Keohane's firewall?

1 A. So it's an illustrative embodiment; right?
2 Because, you know, there are -- you know, Keohane itself
3 says it's one embodiment, but it's a nice embodiment to
4 explain what is going on.

5 Q. And all I'm asking: Am I correct that the
6 embodiment -- all I'm asking is: Am I correct that the
7 embodiment of Figure 7 -- that this process flow shown
8 in Figure 7 can take place within Keohane's firewall?

9 A. I don't see why not.

10 Q. Now, in Figure 7, step 702 asks, "Security
11 policy require security action," question mark.

12 Do you see that?

13 A. Yes.

14 Q. And in Keohane's Figure 7, if the answer at
15 step 702 is yes, then the flow proceeds to a sequence of
16 steps that ends with step 720, add digital signature.

17 Do you see that?

18 A. I see that.

19 Q. And if in step 702 the answer is no, then the
20 process of Figure 7 ends without adding a digital
21 signature.

22 Do you see that?

23 A. I see that.

24 Q. So do you agree that a packet sent by Keohane's
25 firewall may or may not include a digital signature?

1 A. According to this embodiment, the local policy
2 allows to turn off all the filtering.

3 Q. And in this embodiment, that would allow you
4 to -- that would allow the firewall to forward a data
5 packet without adding its digital signature; right?

6 A. It would -- if this is the firewall executing
7 this flowchart, then yes.

8 Q. Is there explicit disclosure in Keohane of
9 Keohane's mail gateway receiving a data packet that was
10 not processed by Keohane's firewall?

11 A. Can you ask the question again?

12 Q. Is there an explicit example in Keohane of
13 Keohane's mail gateway receiving a data packet that was
14 not processed by Keohane's firewall?

15 MR. KLEIN: Object to form.

16 THE WITNESS: I'm afraid I don't remember right
17 now, and it would take a while to read through the
18 patent again. But the whole point here is that I'm only
19 interested in whether or not a redundant operation has
20 already been performed by a trusted element; and if it
21 has, the packet will tell me that and will tell me what
22 operation has been performed, so I can avoid the
23 redundancy. Right?

24 And if for some reason someone has disabled the
25 firewall, I would consider that a feature, not a bug,

1 right, so that means the redundant operation has not
2 been performed. Keohane teaches us how to detect
3 redundant operations and -- from a trusted element and
4 avoid redoing that.

5 BY MR. ZIVOJNOVIC:

6 Q. Sitting here today, can you remember any
7 explicit example in Keohane where a data packet is
8 routed from Keohane's mail gateway to Keohane's
9 firewall?

10 A. From the mail gateway to the firewall.

11 So Keohane is trying to explain how you -- how
12 you avoid redundant operations along one path, and the
13 claims in the patent do the same thing. They only look
14 at packets traveling from one source to one destination.
15 Chandra only talks about packages going from one source
16 to one destination. Right? That's what we're
17 interested in, the things that we touch along the path
18 from a source to our destination and all the security
19 fabric cooperating appliances along the way that may
20 have contributed to establishing security.

21 And so we're interested in the packet along its
22 path. And this is an example path; right? And so the
23 example path has the packets traveling from 306 to 300
24 to 302 to 304. That's the example that we're given.

25 Q. So I believe in your answer you said Chandra

1 only talks about packages going from one source to one
2 destination.

3 You meant Keohane; right?

4 A. So -- so Chandra and Keohane both, in general,
5 in their architecture, describe, you know, traffic, but
6 in order to illustrate the method that they are trying
7 to describe, obviously the method only applies to a
8 single packet or a stream of packets going from one
9 source to one destination, regardless of any other
10 traffic that's going on.

11 That other traffic doesn't -- doesn't apply --
12 you know, individually apply -- that you can apply that
13 I -- but for the purpose of understanding what the
14 method is, you need to look at one packet going from a
15 source to a destination. And that is what all these
16 flowcharts and what, indeed, even the claims of the
17 patent describe. They describe packets on their path
18 from a source to a destination and including all the
19 cooperating security appliances that they touch along
20 that path. That's what we're interested in here.

21 Q. So I just wanted to make sure. I asked you, I
22 think, two questions ago about Keohane; and, in your
23 answer, you mentioned Chandra.

24 And I just wanted to ask: Was that an
25 inadvertent misspeak, or did you intend to reference

1 Chandra?

2 A. I -- I said that both in Chandra and in
3 Keohane, you know, we are talking about a specific flow
4 because we want to explain a mechanism that avoids
5 redundant work along this flow. And that is what even
6 the patent itself -- right, the patent talks about a
7 flow of data packets from source to destination.

8 Q. And in Keohane, the one exemplary flow that's
9 shown is just from the firewall to the mail gateway to
10 the client; right?

11 A. That is the example flow given in Figure 3.

12 Q. And there are no other example flows in
13 Keohane, are there?

14 MR. KLEIN: Object to form.

15 THE WITNESS: Well, I think the background
16 describes, you know, that -- examples where you even
17 have more levels, potentially, where things happen.
18 But, yeah, the example that is given is sufficient to
19 demonstrate the -- the algorithm, especially since
20 the -- in Figure 7, you actually talk about signature
21 headers and adding headers; right?

22 So it's clear -- it would have been clear to a
23 person of ordinary skill in the art that, you know, this
24 could be chained as many deep as you need; right?
25 Because you have incoming signature headers, then you do

1 some processing, possibly avoid redundancy using your
2 local policies, and then in the end, you sign it and say
3 what I -- what you have done. Right? So you can
4 have -- it's clear that you can have many of these.

5 MR. ZIVOJNOVIC: So I would like to enter as
6 Exhibit 1005 a copy of the Buruganahalli reference.

7 (Exhibit Number 1005 marked for
8 identification.)

9 BY MR. ZIVOJNOVIC:

10 Q. Let me know when you've had a chance to
11 download and open that document.

12 A. Okay. Yes. Okay.

13 Q. So if you could please go to Figure 3 in --
14 sorry, let me -- if you could please go to Figure 3 in
15 Buruganahalli.

16 A. Yes.

17 Q. Now, in Buruganahalli Figure 3, traffic is
18 processed first in network device 5 -- 54, then network
19 device 52, and then network device 50; right?

20 A. It looks that way, yes.

21 Q. And there was no disclosure in Buruganahalli of
22 traffic being first processed by network device 50, then
23 52, and then 54, is there?

24 A. That is Figure 3, so let's look at description
25 of Figure 3. It's an embodiment of Buruganahalli.

1 Q. But there's no other embodiment in
2 Buruganahalli where the network traffic flows in the
3 opposite direction, is there?

4 A. It's just an illustration that makes the point
5 of what Buruganahalli is trying to explain.

6 Q. But you're not aware of any examples or
7 illustrations showing traffic going in the opposite
8 direction, are you?

9 A. It's a flow that, again, you have cooperating
10 devices that use these metadata tags to -- to, you
11 know -- to tell you what the previous device did.

12 MR. ZIVOJNOVIC: All right. No further
13 questions.

14 MR. KLEIN: Okay. Let's take a 15-minute
15 break. Let me check my notes. So we can come back,
16 1 -- let's come back at 1:20.

17 MR. ZIVOJNOVIC: Okay.

18 THE WITNESS: Okay.

19 THE REPORTER: Okay. We're off the record.
20 (Off the record.)

21 THE REPORTER: Okay. We're on the record.

22 MR. KLEIN: All right. Dr. Franz, I have just
23 a few questions.

24 THE WITNESS: Okay.

25 ///

EXAMINATION

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

BY MR. KLEIN:

Q. Do you recall opposing counsel asking you questions about whether the '825 patent discloses communications between subnets?

A. I -- there have been so many questions, I do not recall right now.

Q. Well, can I have you pull up the '825 patent, please?

A. The '825 patent. Yes. Correct.

Q. And can you go to Column 4, starting at line 65. Let me know when you're there.

A. Yes.

Q. So the sentence starting on line 65 says, "In this example, a subnet 151 and a subnet network gateway [sic] appliance 150 are connected to private network 120 through the Internet 110 via VPN."

Did I read that right?

A. Yes.

Q. After reading that disclosure, does the '825 patent disclose subnetworks being able to communicate with each other?

A. Apparently it does, yes.

Q. Do you recall opposing counsel asking you questions on whether Chandra disclosed whether traffic

1 received -- or receiving CE could come from something
2 other the transmitting CE?

3 A. Yes.

4 Q. Can I direct your attention to paragraph 96 in
5 your report.

6 A. One second, please.

7 Q. Yes. And I want to point your attention to the
8 sentence starting with "Because." It's the 5th line
9 down.

10 A. "Because each CE label used by the" --
11 (Reporter clarification.)

12 THE WITNESS: "Because each CE label used by
13 the transmitting CE to tag the data packet was
14 registered at the receiving CE, Chandra taught or
15 suggested that when the receiving CE checked the data
16 packet at step 702, the presence of a registered CE
17 label in the data packet indicated that the data packet
18 was transmitted from the transmitting CE, and an
19 unregistered CE label or an absence of a CE label
20 indicated that the data packet was not transmitted from
21 the transmitting CE."

22 BY MR. KLEIN:

23 Q. After reading that paragraph, how would you
24 respond to opposing counsel's questions about whether
25 Chandra disclosed traffic received by receiving CE could

1 come from something other than the transmitting CE?

2 MR. ZIVOJNOVIC: Objection. Vague.

3 THE WITNESS: It -- as I stated, the absence of
4 a CE label indicates that the packet was not transmitted
5 from the transmitting CE. So that would indicate that
6 it's transmitted from somewhere else.

7 BY MR. KLEIN:

8 Q. Do you recall opposing counsel asking you what
9 the, quote, unquote, "next network security appliance"
10 is in your combination of Chandra and Buruganahalli?

11 A. Yes.

12 Q. Can I direct you to paragraph 126 of your
13 report.

14 A. Yes.

15 Q. In this paragraph, are you giving an example of
16 how Chandra combined with Buruganahalli meets claim
17 element 6b?

18 A. I believe I do.

19 Q. And in the example that begins here in
20 paragraph 126 of your report, is Buruganahalli's
21 device 50 the next network appliance participating in
22 the CSF?

23 A. So -- again, so which one is 50? Sorry, I'm --
24 it's been a long day.

25 Q. It's referenced in paragraph 123 of your

1 report, if that refreshes your memory?

2 A. So in 123 -- okay. So network device 50 is the
3 receiving, 52 is the sending.

4 And your question was?

5 Q. You give an example of how you could combine
6 Buruganahalli and Chandra, starting in paragraph 126 and
7 carrying on for the next few paragraphs; right?

8 A. Yes.

9 Q. In that example you give, beginning in
10 paragraph 126, is Buruganahalli's device 50 the next
11 network appliance in element 6b?

12 A. So in this example, we have two cascaded
13 versions of the Chandra -- the Chandra device; right?
14 So the next device is another instance of Chandra.

15 Q. Do you recall opposing counsel asking you
16 questions about which appliances in Keohane were the
17 first and second network appliances?

18 A. Yes.

19 Q. Can I direct you to paragraph 162 in your
20 declaration.

21 A. Okay.

22 Q. After reading paragraph 162, is your mapping of
23 the firewall as the transmitting device and the mail
24 gateway as the receiving device the only mapping for
25 Keohane that you disclosed in your report?

1 A. No. But I believe I stated that in my answer.
2 So the first network could be any network appliance in
3 the appliance chain that received network traffic.

4 Q. And do you recall opposing counsel asking you
5 questions about whether Buruganahalli disclosed traffic
6 going from the Web server to 50 and then to 54?

7 A. What, 50 -- sorry?

8 Q. This is in Buruganahalli's Figure 3.

9 A. Oh, yes. Yes.

10 Q. So you recall those questions?

11 A. Yes.

12 Q. Can I turn your attention to paragraph 49 in
13 Buruganahalli.

14 A. Okay.

15 Q. After reading paragraph 49 in Buruganahalli,
16 how would you respond to opposing counsel's questions
17 about whether Buruganahalli disclosed traffic going from
18 the Web server to 54?

19 MR. ZIVOJNOVIC: Objection. Vague.

20 THE WITNESS: So Buruganahalli states that,
21 "Web server 14 may also send network data 80 to network
22 device 54. In such an example, Web server 14 sends
23 network data 80 first to network device 50. Tag
24 module 72 may be configured to determine that network
25 device 52, the next network device in the chain, is in

1 the set of destinations."

2 Do I need to go on?

3 BY MR. KLEIN:

4 Q. No. So in your opinion, does Buruganahalli
5 disclose traffic going from the Web server to the
6 network device 54?

7 A. It states --

8 MR. ZIVOJNOVIC: Objection. Leading.

9 THE WITNESS: -- it states this quite -- yes.

10 MR. KLEIN: No further questions.

11 MR. ZIVOJNOVIC: No questions from me.

12 THE REPORTER: Mr. Klein, did you want a copy
13 of the transcript?

14 MR. KLEIN: Yes.

15 THE REPORTER: Okay.

16 (The proceedings were concluded at
17 1:33 p.m.)

18

19

20

21

22

23

24

25

1 CERTIFICATE OF STENOGRAPHIC REPORTER
2
3

4 I, RACHEL N. BARKUME, a Certified Shorthand
5 Reporter of the State of California, hereby certify that
6 the witness in the foregoing deposition,

7 DR. MICHAEL FRANZ,
8 was by me duly sworn to tell the truth, the whole truth,
9 and nothing but the truth in the within-entitled cause;
10 that said deposition was taken at the time and place
11 therein named; that the testimony of said witness was
12 stenographically reported by me, a disinterested person,
13 and was thereafter transcribed into typewriting.

14 I further certify that I am not of counsel or
15 attorney for either or any of the parties to said
16 deposition, nor in any way interested in the outcome of
17 the cause named in said caption.

18
19 DATED: January 1, 2024.

20
21 Rachel N. Barkume

22 Rachel N. Barkume, CSR No. 13657, RMR, CRR
23
24
25

Exhibits Ex 1001 Michael Franz 122823 3:13 29:17,19 30:10,12 Ex 1002 Michael Franz 122823 3:12 24:15,17 25:3 Ex 1004 Michael Franz 122823 3:14 39:12,18 Ex 1005 Michael Franz 122823 3:16 72:6,7 Ex 1008 Michael Franz 122823 3:15 57:8,11 Ex A Michael Franz 122823 3:11 18:5,8,16,18,22, 24 19:18 28:9 1 1 19:25 20:6,11 25:11 30:15,18 31:1,3,9 33:20,23 34:12 36:16 39:21 40:13,16 58:22 59:22 73:16 10,084,825 5:23 100 39:22 1001 29:17,19 30:10,12 1002 24:15,17 25:3 1004 39:12,18 1005 72:6,7 1008 57:8,11 102 40:4,21 41:2, 4,11,15,23 42:4,5 43:11,13 53:5 104 39:10	10:02 4:2 110 32:21 74:17 120 74:17 121 20:11 30:19, 22 123 54:23 55:1,5 56:23 76:25 77:2 126 76:12,20 77:6,10 130 30:19,22 14 78:21,22 140 30:19,24,25 140a 31:15,20 36:16 140d 31:16,21 141 32:21,24 141a 31:16,19,24 32:9 36:18 141d 31:16,19,25 32:9 36:23 15-minute 73:14 150 74:16 151 74:15 160 63:2,3,4 162 63:6 77:19,22 166 63:10,12 66:2 1:20 73:16 1:33 79:17 2 2 19:20,23 20:4,16 21:2,8,10,22,25 22:2,21 23:6,13 24:6 25:10 35:18 37:5 41:8,10,13, 21,25 43:7,9 66:22 200 19:23 20:4 2003 28:24 29:2 2020 20:21	2023 4:2 206 43:13 44:8,22 45:12,14,17 208 43:17 44:18 45:1,6,19 49:17, 18,22 21 39:24 40:9 212 43:13 44:9,22 45:12,14,17 214 43:23 44:1,17 45:6,19 48:10,14, 20,24 49:12,17, 19,22 50:24 220 20:10,17 23:7,9,18,20,22 24:10 36:1,4,17, 18,22,24 37:1 38:12 230a 36:5,19,22 230b 36:6,24 37:2 240 38:19 240a 36:12,15,19, 22 38:16 240d 36:24,25 37:2 250 36:6 38:11,20 28 4:1 3 3 12:16 18:14,24 19:1 57:14 59:20 71:11 72:13,14, 17,24,25 78:8 300 57:18,20 58:7,12,21 60:5 69:23 302 57:21 58:14 60:5 63:7 69:24 304 57:25 58:10 60:5 69:24 306 57:17 58:7, 11,13 69:23 32 32:17	33 58:2,6 60:1 34 60:1 35 60:17 63:19 4 4 19:17 74:11 43 33:11 47 47:17 49 78:12,15 5 5 20:9 32:16 72:18 50 25:6,9 55:7,13, 16 56:24 57:3,7 72:19,22 76:21,23 77:2,10 78:6,7,23 52 55:6 57:6 65:10,14,16,18,22 72:19,23 77:3 78:25 53 47:17 48:9,23 54 72:18,23 78:6, 18,22 79:6 58 57:6 5th 58:6 75:8 6 6 54:5,8,10,14 55:4,22 65 74:12,14 6b 76:17 77:11 6th 58:5 7 7 63:12,25 64:3,21 65:1,8,22 66:6,23 67:7,8,10,14,20 71:20 700 66:12	702 67:10,15,19 75:16 72 78:24 720 67:16 8 8 41:18 42:1,2 80 78:21,23 802.11 12:20 802.3 12:13,24 802s 12:15 808 53:11,12,14 814 53:11,12,14 825 5:25 6:3,6,9 19:2,11,20 23:3 25:14,19 27:7,12 29:18 30:12 32:19 34:11 35:7,14,19, 25 38:5 39:1 54:2, 8 74:4,8,10,20 9 9 28:12 96 46:5 75:4 A a.m. 4:2 abbreviation 7:4 12:21 ability 33:5 absence 46:19 75:19 76:3 abstract 10:9,10 abstraction 21:21 accordance 31:6 accurate 5:19 act 53:15 action 63:14,22 64:9,13,15 66:8,
---	--	--	--	---

24 67:11 actions 46:14 47:22 48:11,25 64:11 acts 20:11 23:10 42:21 actual 22:10 34:12 add 56:15 64:13 67:16 added 60:21 64:7 adding 56:1 67:20 68:5 71:21 additional 16:5 address 13:21,25 14:2 66:5 addresses 14:12 55:1,4 afraid 9:15 68:16 agree 7:6 8:10 11:9,23 12:3,24 13:1 14:6 19:10 20:3 21:25 25:22 26:12 29:13 31:1, 8,24 33:21 37:3,5, 15 38:25 46:24 67:24 agreed 5:2,7,12, 16 17:6 40:14,18 ahead 38:23 algorithm 71:19 analog 17:24 analogy 8:8 analysis 61:22 62:3 63:1 analyzed 6:3 26:9 analyzing 6:22 anecdotal 8:16 9:1 answering 5:6 answers 5:1 antennas 11:20	apologies 54:18, 21 apparatus 59:16 apparently 13:24 26:5 47:23 61:18 74:23 appeared 4:5 appears 18:20 20:18 21:18 34:9 36:2 appliance 20:11 23:9 31:20 32:23 33:1,5 43:16,23, 25 52:19 54:10, 15,16 55:2,11,15 57:3 61:23 62:4,9, 12,17,22 63:7,9 74:16 76:9,21 77:11 78:2,3 appliances 19:5, 14,24 20:5 25:11, 15,24 26:13,22 30:19 31:2,10,15 32:22 33:12,19 35:8 36:13 37:8, 23 38:7,8,17 39:1, 7 50:8 69:19 70:19 77:16,17 application 39:11 52:5 53:17 applied 6:22 26:8 45:1 applies 70:7 apply 47:21 64:21,24 70:11,12 applying 49:2 architect 24:9 32:12 architected 59:3 architecture 31:5,8,12,13 32:4, 13 34:9 37:11 70:5 area 20:12 23:10 arrangements 10:18	arrived 20:21 arrives 20:17 23:7,18,20 24:3 36:1 53:1,5 arriving 52:18 art 6:7,13,22 7:9, 13 26:9 27:24 51:24 57:9 61:13 71:23 asks 67:10 assign 14:12 assume 5:15 attention 75:4,7 78:12 authenticate 47:7 64:6 authenticated 47:9 avoid 19:6,15 44:13 50:1 60:12 61:1,2 64:16 68:22 69:4,12 72:1 avoiding 44:21 51:9 avoids 33:14 71:4 aware 5:20 9:3,4 35:13 73:6 B back 28:9 59:24 61:25 66:2 73:15, 16 background 71:15 backtrack 17:4 Barkume 4:3 base 11:20 based 28:15 33:6 62:13 64:10 basis 51:14 beginning 58:11	77:9 begins 76:19 behalf 4:7 big 24:19 bingo 14:4 bit 15:6 23:5 26:24 Black 16:19 bother 52:3 bottom 25:13 boundaries 40:24 box 11:5 42:5 boxes 9:25 14:23 22:18 30:21 39:5 branch 23:13 24:5 36:5,6,19,24 37:7 branches 37:16 break 29:24 30:2 53:19 73:15 broke 54:19 brought 26:25 27:3 bug 68:25 buildings 8:7 built 16:14 Buruganahalli 55:5,17,23,24 56:7,12 57:5 72:6, 15,17,21,25 73:2, 5 76:10,16 77:6 78:5,13,15,17,20 79:4 Buruganahalli's 55:13 56:24 57:2 76:20 77:10 78:8 C cable 11:5 13:8, 11,15,20,23 14:4, 7,16,19,24	cables 8:6 9:25 22:18 California 4:4,5 called 4:7 10:14, 16 15:4 40:21 62:10 calls 31:18 34:20 carrying 77:7 cascaded 77:12 cascading 46:3 case 12:3 14:23 37:13 39:5 46:24 47:21 49:7,9,11 60:19 CE 46:13,19,21 47:1,2,8,11,14,19, 20,21,24 48:1,7, 10,14,20,24 49:4, 8,12 50:13,24 51:1,4 52:13 53:6, 7 75:1,2,10,12,13, 14,15,16,18,19, 21,25 76:1,4,5 Certified 4:3 CES 47:4 chain 56:5,14 63:9 78:3,25 chained 71:24 chance 18:11 30:9 39:15 72:10 Chandra 39:11, 19,21 41:2,5,7 42:6 43:14,21 44:4,7,12,16,20 45:4,15,16,24 46:3,24 47:13,16, 18,21,23 48:1,3,5, 9,19 49:11 50:1, 11,20,23 51:7 52:12 55:23 59:5 69:15,25 70:4,23 71:1,2 74:25 75:14,25 76:10,16 77:6,13,14 Chandra's 40:2, 12,16 41:10,13, 17,20 42:2 43:6,9
---	---	---	--	---

44:1 check 73:15 checked 75:15 cites 28:22 citing 20:7 27:24 29:9 35:10 claim 6:9,17 43:22 54:5,8,10, 14 55:4,11,15,22 62:24 76:16 claimed 43:15 62:16,21 claims 28:1 46:4 50:5 62:10 69:13 70:16 clarification 5:15 75:11 clarify 5:11 11:21 clause 46:17 clear 4:23 7:10,11 15:24 71:22 72:4 client 57:23,25 60:5 71:10 clients 58:23 close 29:22 closer 43:6 clothing 8:1,13, 23 9:7,10,15,20, 24 collaboration 50:8 collaborative 65:5 collection 40:4 Column 32:16 74:11 combination 37:19 76:10 combinations 37:7 combine 77:5 combined 76:16	combining 55:22 commencing 4:2 communicate 13:11,16 14:20 44:14,24 74:21 communicated 47:5 communicating 13:14 49:21 58:23 communication 51:14 communication s 74:5 complicated 10:17 component 45:22 52:14 compound 7:15 26:2 56:3 comprise 31:25 32:1 computations 15:10,11 computer 8:4,21 9:2 10:3,5,11,22 11:9,23 17:14,15, 17,22 computers 10:6, 12 11:11,17,25 13:2,8,10,17,19, 24 14:7,9,13,15, 18 17:7,9,10,13, 18 31:25 32:10,15 computing 15:1, 5,8,9,15 16:3,10 31:21 concerned 51:7, 8 53:9 concluded 79:16 Conferencing 4:3 confident 49:22 configure 14:8	configured 14:19 57:6 78:24 confirming 24:25 connect 13:7,10, 19 14:4,7,12,18 31:20 connected 7:21 10:12,16,20 13:17 14:15 17:9,10,13 22:19 34:10 38:11,14,16 41:14,22 42:3 43:2,5 74:16 connecting 13:22,24 connection 5:22 13:4 14:8 15:14 16:19 42:23 47:10 connections 42:13 connectivity 11:8,10,24 12:2, 11 connects 10:6, 11,14 20:12 21:21 23:10,22 consist 17:7 consistent 16:6 28:18 29:16 consistently 62:19 consists 14:15 19:24 20:5 constituent 11:11,25 construct 6:25 consumer 49:10 contemplates 47:23 contend 57:2 context 7:10,17 8:11,13 15:1,2,21, 22,24 16:2,10 25:18 27:7,17 38:4,25	contributed 69:20 convenient 29:24 cooperate 21:16 26:17 44:14 65:4 cooperating 26:21 50:7 52:1, 19 56:20 59:16 62:11 64:7,18 69:19 70:19 73:9 cooperation 49:3 50:9 64:25 65:1 cooperations 65:2 cooperative 6:10,13,17,23,25 7:2,4,6,9,15 19:4, 13,23 20:4,20 21:2,8,10,15,17 22:22 23:4 26:4 27:22 33:13,20,24 55:18 59:9 64:18 65:6 coordinate 19:5, 14 25:23 26:22 27:21 coordinated 27:17 coordinates 33:13 coordinating 25:15 26:6,12 coordination 49:2 copy 18:6,21 24:16,25 25:3 28:9 29:17 30:12 39:11,18 54:2 72:6 79:12 core 64:16 corporate 32:14 correct 6:3,4,7,8, 14 29:8 43:15,20, 22 45:7 46:1 55:24 57:25 64:21	65:20 66:21,22,23 67:5,6 74:10 correctly 65:25 correspond 36:16 corresponds 20:10 23:9 36:13 62:22 coughed 54:21 counsel 74:3,24 76:8 77:15 78:4 counsel's 75:24 78:16 court 4:22 create 4:23 12:1 creating 4:22 crossbar 10:17 cryptographic 42:18 CSF 7:3 19:4,13 25:14,20,23 26:4, 8,11 54:11 55:3,8, 12,16 56:25 57:4 76:22 current 28:15 customary 28:18 29:11,14 customer 43:16, 23,24 44:1,17,18, 19,24 45:6,9,10, 18,19,22,25 48:17 51:11 53:2,3 D dangerous 42:21 data 7:17 8:11 17:15,16 46:11,20 47:19,22 48:10, 12,13,25 49:1 57:6,17,20,25 58:7,11,13,19,20 60:4,15,17 63:22 65:24 66:13 68:4, 9,13 69:7 71:7 75:13,15,17,20
--	--	---	--	--

78:21,23	describing 60:25	direct 75:4 76:12 77:19	edge 43:16,23,24 44:1,17,18,19,24 45:6,9,10,19,22 48:17 49:10 51:11 53:2,3	47:15
day 76:24	description 34:12 72:24	direction 73:3,8	edges 45:18 46:1	establishing 9:6 69:20
December 4:1	design 35:5	directly 7:20 10:12,14,16,21 13:8 38:12	educated 9:7	ethernet 12:19, 22 13:1,4,8,11,12, 14,18,20,23 14:7, 16,19
decide 49:23	designed 24:8 37:21	disabled 68:24	elect 51:16 53:12 60:22 62:12	EXAMINATION 4:10 74:1
decision 16:25 18:6,18 28:10	designer 35:4	disclose 44:16 47:13 48:1,6,19 60:14 74:21 79:5	element 59:16,18 60:19 61:12 63:19,20 65:23 66:12,25 68:20 69:3 76:17 77:11	examine 64:4
declaration 6:5, 12 16:18 24:16 25:1,4,7 43:19 46:6 54:24 66:3 77:20	destination 24:12,14 27:1,6,8, 16 28:3,5 36:7,8 37:6,16,19,25 38:2,3,6 39:3,8 69:14,16,18 70:2, 9,15,18 71:7	disclosed 55:6 57:5 74:25 75:25 77:25 78:5,17	elements 59:8,15 63:15 64:18,25 65:5 66:8	examined 4:9
deep 71:24	destinations 79:1	discloses 6:13 48:3 74:4	embodiment 31:6 39:22 65:12, 17 67:1,3,6,7 68:1,3 72:25 73:1	examines 60:17
define 25:20 27:1 33:15	destined 24:4 36:4,18,23 38:15	disclosure 58:18 61:6 68:8 72:21 74:20	embodiments 33:11,18	examples 34:16, 17 35:3,8,13 47:13 71:16 73:6
definition 16:21 29:13	detail 12:22	discussed 17:5	end 32:9,15 41:14,21,22 42:3 43:10,11 44:6 64:13 72:2	execute 33:6
demonstrate 71:19	detect 53:14 69:2	discussion 52:23	endpoint 38:14, 15	executing 68:6
depend 37:25 39:3	determination 61:10	dissect 56:3	ends 44:14 67:16, 20	exemplarily 35:11
dependent 46:3	determine 60:18 78:24	distributed 15:1, 5,7,9,15 16:2,10	ensure 48:12	exemplary 31:5 71:8
depending 23:14 37:5,15,19 38:6, 10 39:8 40:22 49:25	determined 58:12	document 18:12 39:16 72:11	entity 64:7	exhibit 18:3,5,8, 16,18,22,24 19:18 24:15,17 25:3 28:9,24 29:2,17, 19,23 30:10,12 39:10,12,18 57:8, 11 72:6,7
depends 24:7 32:11 35:5 38:3	device 17:24 52:2,7,8 55:6,7,8, 13,16,19 56:6,14, 21,24 57:3,6,7 72:18,19,22 73:11 76:21 77:2,10,13, 14,23,24 78:22, 23,25 79:6	dot 12:16	environment 31:22 39:22 40:12,16	exhibits 29:5
depict 22:21	devices 50:7 55:25 56:1,4,17, 19,20 62:7 64:14 73:10	download 18:12 30:10 39:16 72:11	essential 44:11	existing 13:14
depicted 63:13 66:7	dictionary 16:22 28:22,25 29:3,8, 10,14	downloading 24:24	establish 14:8 36:10 42:19 47:5	expert 9:14,23 63:4
depicting 21:20	difference 21:12, 14	downstream 32:20 33:25 34:13,21 35:25 64:15	established 23:22 47:12 51:13 52:1,7	explain 15:2 20:19 64:24 65:1, 2 67:4 69:11 71:4 73:5
depicts 21:2,8 25:10 31:1,3,4,7 66:23	differs 38:10	draw 40:23	establishes	explains 44:4 65:4
deployed 13:5	digital 67:16,20, 25 68:5	drill 26:24		explanation 61:5
deposition 4:23 5:21		duly 4:8		explicit 61:6 68:8,12 69:7
describe 16:12, 13 59:14 60:11 70:5,7,17		E		explicitly 50:12 60:3,14
describes 19:2, 11 25:14 27:23,25 35:25 60:3 61:10 71:16		e.g. 46:12 63:15 66:8,12,16,19,25		expresses
		earlier 11:21		

22:17,20 expressly 48:6 external 27:18 31:21 F fabric 6:10,14,17, 24 7:1,2,4,6,8,12, 15,16,18,24,25 8:1,11,12,17,21 9:10,20,25 11:1,2, 3,8,18,19 12:4,8, 11 14:20,23,25 15:13,16,20,21, 23,24 16:2,9,11, 21 19:4,13,24 20:5,20 21:3,9,11, 15,16,17,18 22:5, 7,10,12,15,17,18, 22 23:4 26:3,16, 21 27:22,23 28:16 29:11,15 33:13, 20,24 50:7 59:9 64:19 69:19 fact 51:21 61:9 fair 6:16 10:22,24 35:7 42:24 52:14 55:12 58:18 63:25 familiar 12:13,21, 22 13:7 feature 68:25 field 15:4 fields 16:12 figure 19:20,23, 25 20:4,6,11,16, 18 21:2,8,10,22, 25 22:21 23:6,13 24:6 25:10,11 30:15,18 31:1,3,9 33:20,23 34:12 35:18,22 36:16 37:5 39:21 40:13, 16 41:8,10,13,18, 21,24,25 42:1,2 43:7,9 57:14 58:22 59:20,22 63:12,25 64:3,21 65:1,8,22 66:6,11, 22,23 67:7,8,10,	14,20 71:11,20 72:13,14,17,24,25 78:8 file 24:19 filtering 68:2 final 46:17 find 37:12 finish 4:24 5:1 firewall 57:18,20 58:7,12,21 60:4, 16,21 61:22 62:3, 8 63:20 64:1,23 65:2 66:25 67:8, 25 68:4,6,10,14, 25 69:9,10 71:9 77:23 five-minute 30:2 flag 30:1 48:16 49:19,21 51:14,15 52:19,22,25 53:15 55:7 59:17 62:13 flags 51:23 52:23 64:12 flow 63:13 66:7, 24 67:7,15 71:3,5, 7,8,11 73:9 flowchart 52:21 57:19 59:3 64:4 68:7 flowcharts 70:16 flows 71:12 73:2 focuses 43:12 form 6:18 8:2,14, 25 10:4 11:10,12, 24 12:2,5 13:3 20:23 21:4 22:9, 23 23:25 26:14 27:10 30:20 33:13,20 37:9 40:19 51:3 60:8 61:24 65:3 68:15 71:14 Fortinet 16:23 Fortinet's 16:15 forward 68:4	forwarded 36:5 forwarding 44:16 forwards 57:20, 25 found 6:13 Franz 4:6,14 30:9 73:22 full 4:12 5:19 function 51:2 functionality 45:11,23 46:1 functioning 40:6 functions 7:12 40:13,17 41:3,4 49:10,13 50:24 51:5 52:14 65:6 G gateway 57:21, 22,24 58:13 60:5, 17,21 62:11,17,23 63:7,15,20 64:2, 22 66:9,13,16,20 68:9,13 69:8,10 71:9 74:16 77:24 general 27:25 64:4 70:4 gentleman 59:13 give 5:4 14:2 25:20 77:5,9 giving 61:2 76:15 good 53:19 ground 4:17 guarding 36:13 guess 9:5,7 36:10 38:23 H handles 42:15 handshake 47:6	happen 50:3 71:17 happened 49:16 happening 15:11 45:2 59:11,21 61:3,8 happy 5:11 29:25 header 56:1,2 64:6,11 headers 44:23 64:5 71:21,25 heard 14:25 15:13 hierarchical 31:11 historian 9:2 hops 38:19 hour 29:22,23 53:19 I i.e. 32:22 idea 8:6,22 identification 18:9 24:18 29:20 39:13 57:12 72:8 identified 46:13 identify 45:24 47:10 64:5,9 IEEE 12:13 illustrate 70:6 illustrated 65:22 illustrates 39:21 60:9,10 illustration 59:5, 20 73:4 illustrations 73:7 illustrative 59:3, 5 65:16 67:1 image 19:20	implemented 65:23 implementing 39:22 implies 50:15 52:17 60:23 imply 52:23 important 4:24 5:4 inadvertent 70:25 include 32:9,15 35:8 67:25 included 49:19 including 70:18 incoming 23:6, 12,15 39:2 51:18 71:25 individual 36:14 40:5 individually 70:12 information 35:3 56:10,11 infrastructure 8:17 10:1,6 12:11 15:19,25 16:13 21:19 22:11 42:21 initially 58:21 inside 42:5,16 inspired 8:5,12, 22 instance 45:25 77:14 instances 52:12 institution 16:25 18:6,18 28:10 intend 70:25 intending 42:1 interconnected 40:5 interconnectedness 7:22
--	--	---	---	--

interested 28:2 68:19 69:17,21 70:20	68:8,12 69:2,7,11 70:3,4,22 71:3,8, 13 77:16,25	learned 64:10	matter 61:4	moving 29:23		
interfere 18:3	Keohane's 61:22 62:3,17,22 63:14, 25 64:1,22 65:2 66:8,25 67:8,14, 24 68:9,10,13,14 69:8	leaves 37:16,22	matters 9:8	multiple 14:1 15:10 26:16 50:7 59:8		
intermediaries 10:19		level 11:2 37:3	meaning 6:23 7:2,7,16 9:18,19, 24 12:9 26:2,18 28:18 29:11,15 45:8	multiple-level 60:10		
intermediary 63:21		levels 71:17				
Internet 20:13 23:11,23 24:4 27:8,13,18 32:21, 25 33:25 34:2,7, 14,15,19,23 35:12 36:4 37:6,18 38:15 39:2 42:14 44:2 46:12,25 48:2,8,11,15,21, 25 49:12 50:18,23 74:17	kid 17:20	light 6:6	means 9:20 16:9 22:5 38:5 51:15 60:21 61:18 66:19 69:1	N		
interpret 28:16	kind 50:15	limitation 55:1	meant 7:14 70:3	names 4:15		
invalidity 6:6 43:14,21 45:4 61:22 62:3,21	Klein 6:18 8:2,14, 24 9:13,22 10:4 11:12 12:5,14 13:3 17:23 20:23 21:4 22:9,23 23:25 26:14 27:10 30:20 37:9 40:19 44:3 51:3 52:15 53:18 60:8 61:24 62:5 65:3 68:15 71:14 73:14,22 74:2 75:22 76:7 79:3,10,12,14	links 11:14	mechanism 71:4	naming 27:5		
invention 31:7 33:11,18 39:23 59:13		local 33:6,15 49:25 68:1 72:2	meets 76:16	negotiate 14:3		
involved 38:9		located 7:23	members 33:14	network 7:17,19, 20 8:11 10:1,3,5, 8,9,22,23,25 11:9, 15,17,23 12:2,4,9 13:5 14:4,13,14, 22 17:6,9,17 19:3, 4,12,13,24 20:5, 11,12,13,17 22:8 23:9,10,11,23 24:4,8,9 25:10,16, 24 26:6,13,25 27:2,9,18,20,25 28:16 31:2,4,5,8, 9,12,14,15,20 32:14,20,22,23 33:1,4,5,12,19,25 34:1,9,13,14 35:4, 6,8 37:7,21,23 38:1,6,8,17 39:1, 21 40:4,6,12,13, 16,17,20,22 41:2, 3,4,5,11,15,22 42:4,5,8,11,12 43:3,10,11,16,22, 25 44:11 45:13,25 47:13 50:4 53:5 54:10,14,15,16 55:2,6,7,11,13,15, 16,19 56:24 57:3, 5,6,7 58:22 59:1, 2,12 61:4,23 62:4, 11,16,22 63:7,8, 19 65:24 72:18, 19,22 73:2 74:15, 17 76:9,21 77:2, 11,17 78:2,3,21, 23,24,25 79:6	mentioned 48:23 70:23	network.' 28:17
IP 13:21,25 14:2, 12		lost 59:24	memorized 32:7			
IPR 5:22 18:4 24:16		lot 12:15 14:10 52:22	memory 77:1			
Irvine 4:5		lots 10:12 14:3 15:17	mentioned 48:23 70:23			
issue 26:25			mentions 35:11 48:23			
issued 17:1 18:6			metadata 55:21 56:4,9,14,18 73:10			
			method 44:12,21 59:4,6 60:11,25 70:6,7,14			
			methods 19:2,11			
			Michael 4:6,14			
			middle 4:14 10:13 32:23,25 33:12,19 40:21 56:9,17			
			mind 24:24			
			minimum 8:10 25:22			
			missing 53:15			
			misspeak 70:25			
			modified 55:21			
			modify 42:17			
			module 78:24			
			move 18:2 23:4 28:8			

networked 17:18 networking 8:5, 18,22 9:25 12:10 13:2 15:22,25 34:6 51:8 networks 20:13 23:11,23 24:3 34:4 40:5 Newton's 16:22 28:22 29:2,10,13 nice 67:3 nodding 5:5 node 20:10 23:22 nodes 23:13 24:5 38:1 non-secure 46:13 nonverbally 5:6 notes 73:15 number 5:22 24:17 29:19 39:1, 4,12 57:11 72:7 numbers 18:4 39:6 numeral 25:20 O oath 4:19 16:4 object 6:18 8:14, 24 9:13,22 10:4 11:12 12:5,14 13:3 17:23 20:23 21:4 22:9,23 23:25 26:14 27:10 30:20 37:9 40:19 44:3 51:3 60:8 61:24 65:3 68:15 71:14 objection 8:2 52:15 62:5 76:2 78:19 79:8 objective 26:5,15 observes 42:15 occasionally 7:3	occurring 15:10 office 17:1 18:7 19:1,19,22 20:3 28:14,21 29:9 office's 19:10 Ogi 53:18 Oliver 4:15 open 57:10 72:11 operating 59:7 operation 27:17 55:20 59:18 64:1 68:19,22 69:1 operations 19:3, 5,6,12,14,15 25:15,23 26:6,12, 22 33:6,14,15 35:15 44:13,21,25 48:18 49:5,22,23, 24 50:2 51:17 52:9 60:12,22 61:1,3 62:13 64:17,19 69:3,12 opined 6:12 opinion 79:4 opposing 74:3, 24 75:24 76:8 77:15 78:4,16 opposite 73:3,7 order 10:18 12:1 70:6 ordinary 7:1,13 26:2,18 28:18 29:10,14 51:24 61:13 71:23 originated 46:12 48:2,21 originates 50:22 originating 46:25 48:7 out- 27:18 Owner 4:7 16:15 P p.m. 79:17	package 62:9 packages 69:15 70:1 packet 38:2 44:22,23 46:11, 13,14,20 47:19,22 48:10,12,13,25 49:1,16,19 50:6 51:19 55:20 56:21 57:17,20,25 58:7, 11,13 59:14,15 60:4,15,18 63:22 66:13 67:24 68:5, 9,13,21 69:7 70:8, 14 75:13,16,17,20 76:4 packet along 69:21 packets 28:2 44:8 45:12 53:10 58:19,20 59:2,7 69:14,23 70:8,17 71:7 pair 47:3 paragraph 25:6, 9,13 28:22 39:24 40:9 46:5 48:9,23 50:14,17 54:23 55:1,5 56:23 58:2, 5,6,10 59:25 60:1 63:2,3,4,10,12,19 65:10,14,18,22 66:2 75:4,23 76:12,15,20,25 77:6,10,19,22 78:12,15 paragraphs 77:7 part 7:20,21 10:10 39:8 partially 49:24 participating 54:11 55:2,8,12 56:25 57:4 76:21 parties 18:5 parts 7:11,23 15:11 26:20 45:20,21 party 42:15 51:12	pass 37:1,20 56:12 passed 51:25 58:13 passes 37:22 50:6 passing 19:3,12 25:16,24 26:7,13 59:8,15 patent 4:7 5:22 6:1,3,6,9 16:15 17:1 18:6 19:1,2, 10,11,19,20,22 20:3,7 22:2,25 23:3 25:14,19 27:7,13,23 28:14, 21 29:9,18 30:12 31:18,19,22 32:4, 19 33:22 34:11 35:7,14,19,25 38:5 39:1,11 49:16 53:16 54:3, 8 59:4 62:10 68:18 69:13 70:17 71:6 74:4,8,10,21 path 33:5 38:9 39:7 44:5,9 51:18 53:13 57:22 61:17,19,20 69:12,17,22,23 70:17,20 paths 37:20 51:24 Perfect 63:5 perform 51:5 65:5 performed 25:16,23 26:13 46:14 49:6 56:18 63:21 64:11 68:20,22 69:2 performing 19:2, 11 35:14 63:14 66:7,24 performs 48:11, 25 49:13 50:24 51:2 52:14 perimeters 31:16	person 7:13 10:18 51:23 61:13 71:23 perspective 42:25 phrase 8:12 14:25 15:13 physical 7:18,22 8:17 10:1 11:7,10, 24 12:9,10 13:14 15:18 16:13 21:18 22:11,12 28:17 45:20 physically 11:3 14:7 22:19 picture 21:5,19 22:2 58:1 61:16 piece 9:10 54:9 place 59:8,25 67:8 places 15:10,12, 17 plain 7:1,7,16 9:17,19,24 26:1, 18 plugged 11:6 12:7 point 5:9 11:22 22:11 27:1 34:9 36:3 52:17 56:16 62:24 64:17 68:18 73:4 75:7 pointing 45:14 55:13,16 62:17 63:6 policies 33:7,15 49:25 72:2 policy 67:11 68:1 pops 24:24 position 48:5,19 50:11,25 possibility 51:22 possibly 72:1 potentially 42:21 71:17
---	---	---	--	--

precisely 48:15	provided 46:2	78:15	redundant 19:6, 15 33:14 44:13,21 48:18 50:2 51:9 60:12 61:1,2 62:12 64:16 68:19 69:1,3,12 71:5	require 67:11
prefer 29:25	providing 45:10	real 22:17,20		requires 11:10, 24 12:10 26:12 54:8,10 55:2
preliminary 16:16	public 42:13	realize 11:3		research 16:5
presence 75:16	publications 4:16	realized 42:14		respond 75:24 78:16
present 31:6 32:20 33:11,18 39:23 60:19 61:12,15 64:12	pull 74:8	realizes 22:19	refer 5:25 8:17	responding 4:25
previous 25:18 49:10 52:7 64:10 73:11	purpose 15:19 26:17,21 37:11 70:13	reason 5:18,20 68:24	reference 7:25 12:18 25:20 57:9 70:25 72:6	response 16:16
previously 18:21 47:4,11 49:18 51:12,25 52:1	purposes 24:23 42:22,24	recall 74:3,7,24 76:8 77:15 78:4, 10	referenced 76:25	responses 5:4
prior 6:6,13,22 26:9 27:24 57:9		receive 44:2 48:7,14,20	references 41:11	responsible 37:17,24 39:2
private 20:12 23:11,23 24:4 27:9 32:14 42:8, 11,12,19,22 43:3 74:16	Q	received 36:3,17 44:17 46:25 50:18 57:18 58:7,20 60:15 66:13 75:1, 25 78:3	referring 15:3	rest 44:10
proceeding 16:16,19,23 17:1 18:7,19 24:16 28:15	qualified 15:23	receiver 17:15 53:10	refers 22:7,10	result 25:15
proceedings 79:16	qualify 11:1	receives 48:10, 24 49:11 62:9	reflects 29:14	review 18:12 30:10 39:16
proceeds 67:15	question 5:1,9, 14 11:21 14:5 19:7 21:6 27:4 28:6 38:24 40:15, 25 42:1 47:25 50:16 55:14 62:1, 20 67:11 68:11 77:4	receiving 17:16 41:14,22 42:3 43:10,23,24 44:1, 6,17,24 45:6,10, 19 46:13 47:1,4, 20 48:1,7,10,14, 20,24 50:13,23 51:11 53:2,6 68:9, 13 75:1,14,15,25 77:3,24	refreshes 77:1	reviewed 16:15, 17,18,21,25 18:21
process 24:20 34:25 38:7 63:13 65:22 66:7,24 67:7,20	question's 64:20	recognizable 47:20	registered 75:14, 16	revisit 17:4
processed 23:12 24:5 33:24 45:5,9, 18 50:13 52:13 68:10,14 72:18,22	questions 4:25 5:5 70:22 73:13, 23 74:4,6,25 75:24 77:16 78:5, 10,16 79:10,11	recognize 18:16 25:3 29:2 39:18	relates 12:19	rig 13:13
processes 20:21	quick 43:19 65:9	recognized 46:11	relating 5:22	role 20:12 23:10
processing 35:9 37:17,24 38:16 39:2 56:21 65:24 72:1	quote 63:18 76:9	record 4:13 24:23 28:16 30:6,7 53:22,23,24 73:19,20,21	relationship 47:12 51:13 52:8	root 20:10,17,21 23:7,9,18,22 32:22,25 33:12,19 36:1,4,5,17,18,24 38:12
prove 52:6	quoting 47:16	redoing 69:4	relevant 50:5	rotating 35:22
provide 5:19 50:12	R	reduce 50:9	relying 45:5,17	route 36:7,21 42:20
	Rachel 4:3	redundancy 50:9 68:23 72:1	remember 32:2 68:16 69:6	routed 69:8
	re-ask 41:25 62:20		REMEMBERED 4:1	router 63:20
	read 50:14,17 54:9 65:25 68:17 74:18		remote 43:1	routers 39:5
	reading 31:22 39:23 40:3 60:23 74:20 75:23 77:22		remotely 4:5	routes 36:20 37:22
			remove 56:16	rule 4:24
			repeat 21:6 28:7 59:18	rules 4:17 44:25 48:12 49:1
			rephrase 5:11 11:21 14:5	S
			report 63:4 75:5 76:13,20 77:1,25	safe 48:13
			reporter 4:4,22 53:22,24 73:19,21 75:11 79:12,15	sanity 35:22
			reproduced 19:19	

scenario 51:1	74:14 75:8	sitting 8:20 16:8 69:6	40:2 41:6 47:25 50:19 58:17,19 66:5	switch 17:4 28:17
science 8:4,21 9:2	sentences 40:3	situations 52:24 60:24 61:14		sworn 4:8
scientifically 9:5	separate 56:1	skill 7:13 51:24 61:13 71:23	started 4:18	system 45:2 60:10 64:8 65:24
scope 6:17,19 8:24 9:13,22 12:14 13:3 17:23 20:23 44:3	separates 31:21	skills 61:13	starting 32:17 33:10 74:11,14 75:8 77:6	
scroll 19:17	sequence 44:8 45:11 56:3 67:15	skip 38:22 49:24	starts 34:18,22	T
secret 47:6	server 60:15 61:19 78:6,18,21, 22 79:5	slight 21:20	state 4:4,12	tag 55:21 56:9,10, 14,18 75:13 78:23
secure 42:14 48:13	servers 58:23	software 14:1	stated 76:3 78:1	tagged 47:19,20
security 6:10,14, 17,23 7:1,2,4,6, 10,12,15,17 8:12 19:3,4,5,6,12,13, 14,15,23,24 20:4, 5,11,20 21:2,8,11, 15,16,17 22:22 23:4 25:15,23 26:3,6,12,17,21, 22 27:17,22 31:2, 9,15,20 32:22,23 33:1,5,6,7,12,13, 19,20,24 35:8,14 36:13 37:8,23 38:7,8,17 39:1 43:16,23,25 44:25 45:10,23 46:1 49:10,13 50:7,10, 24 51:2 52:2,14, 19 54:15 55:20 59:9,16 60:10,12, 19,22 61:11,23 62:4,9,16,22 63:7, 14,19,21,22 64:9, 11,18 65:6,23 66:8,12,24,25 67:10,11 69:18,20 70:19 76:9	set 37:23 38:1,6 46:14 47:22 79:1	solely 14:15	statement 19:10	tags 56:2 73:10
	setup 44:22 47:9	solutions 13:13	states 22:2,25 78:20 79:7,9	takes 44:5
	shared 47:6	sort 8:5	stating 56:23	talk 10:18 24:12, 13 71:20
	Shorthand 4:4	source 24:13 27:1,5,8,13,16 28:3,5 37:19 38:2 39:7 58:12 69:14, 15,18 70:1,9,15, 18 71:7	stations 11:20	talked 23:6 62:6
	showed 61:17	special 49:21 56:8	step 66:12 67:10, 15,16,19 75:16	talking 7:11 15:21,24 23:15, 17,19 24:11 27:12 32:4 34:13 47:3 49:15 51:21 71:3
	showing 73:7	specific 24:8 27:3,4 28:2 31:4 32:11 38:18 47:3, 8,11 51:8 53:9 59:4,6,7 61:4 62:24 63:1 71:3	Stephen 4:15	talks 35:14 47:18 48:22,24 49:2 69:15 70:1 71:6
	shown 24:6 25:11 36:10,12 67:7 71:9	specifically 23:19 34:13 38:5 44:7,20 49:15 50:21	steps 67:16	target 38:10
	shows 19:23 20:4 21:10,22,25 22:2 31:9,11 43:9 58:1, 22 63:25 64:3	specification 22:4,25 31:23 32:2,3,4,7 33:22 35:10,16 48:22	stream 37:12 70:8	taught 75:14
	sic 20:21 39:10 41:21 58:10 74:16	stage 28:15	streams 28:2	TCP/IP 14:8,20
	sic] 33:7	standard 12:23, 25 13:1,12,18	structure 7:18 12:9 28:17	teach 52:16
	sign 72:2	standards 13:15	submitted 6:5 16:16,18,22 18:4	teaches 47:21 52:12 53:16 56:12,13,15 60:4 69:2
	signature 60:18, 25 61:11,21 64:5, 14 67:16,21,25 68:5 71:20,25	stands 42:8	subnet 31:20,21 32:21,23,24,25 33:12,19 34:1,5,8, 19,22 35:12 36:18,23 74:15	teaching 52:6,10 64:24
	simple 12:7 17:8	star 10:14	subnets 31:16, 19,24 32:9,14 34:14,15 35:1,9, 15 36:14 74:5	teachings 64:21
	simpler 47:25 64:20	start 7:24 12:25 17:3 18:15 21:13 22:5 23:21 30:15 36:11 37:4 38:14	subnetworks 74:21	technique 51:9
sees 62:13	simply 25:14		subscript 15:20	technology 13:5 42:19,25
send 57:6 78:21	single 40:6,13, 17,22 41:3,5 49:12 50:13,23 52:13 70:8		sufficient 71:18	Telecom 16:22 28:22 29:3,10,14
sending 17:15 77:3	sir 18:13 25:2 50:16		suggested 75:15	telling 44:12 51:7,10,20 59:19
sends 78:22			supposed 24:10	tells 10:10,20 44:7,20 49:21 50:1,4 51:14
sense 32:13			suppress 62:12	
sentence 25:19 33:4 40:10 46:10, 18 65:21 66:11				

55:24 61:12 65:16	touched 38:2	traveling 28:3 44:22 45:12 69:14,23	user 31:25 32:9, 15	work 50:10 51:9 53:12 65:2 71:5
term 6:17,23,25 7:2,8,15 8:4,16,21 9:4,6,8 16:2,11 25:20 26:1,2 42:6	trade 47:7	traverse 36:18, 24 37:6	V	works 37:18 64:25
terms 6:9 9:3 15:21	traffic 19:3,12 20:16,21 23:7,12, 14,16,17,20 24:3, 5,7,10,12,13 25:16,24 26:6,13, 25 27:2,8,12 32:20,24 33:23,25 34:1,3,4,7,13,15, 17,18,22,25 35:4, 9,11,15 36:1,3,9, 17,23,25 37:6,12, 15,17,21,24 38:7, 15 39:2,3 42:15, 16,20 43:10,12 44:2,5,17 45:5,13, 17,25 46:12,25 47:1,10,14,23 48:2,3,7,15,16,20 49:3,12 50:12,18, 22 51:11,12,22 52:13,18 53:1,5 55:7 62:14 64:15 70:5,10,11 72:17, 22 73:2,7 74:25 75:25 78:3,5,17 79:5	traverses 45:25	Vague 76:2 78:19	world 22:18,20 36:21,25 38:9
testified 4:9 34:24		tree 37:13 39:8	verbal 5:4	wrap 57:24
testify 4:8		tree-shaped 31:12 37:11	versions 77:13	write 25:9,12,14 40:8 46:11,16 55:5 66:6,12
testimony 5:19		true 5:19	versus 21:15	written 4:22 19:8, 9
text 19:8,9		trusted 58:12 60:19 61:11 63:19 68:20 69:3	Video 4:2	wrote 19:2,22 25:21 28:14 46:18 55:10 57:1 63:12 66:10,16,18
theory 34:24 61:7,9 62:21		truth 4:8,19	view 10:25 14:14, 18 21:12,14 22:5, 7,15,21	
thereof 4:2		tunnel 42:14,16, 17,20	virtual 42:8,11,12 43:2	Z
thing 10:10,13 22:12 69:13		turn 68:2 78:12	VPN 42:6,8,25 74:17	
things 11:6,7,20 12:7 14:3,10 22:13 26:16 34:10 49:3 50:5 69:17 71:17		type 17:21	W	ZIVOJNOVIC 4:11 6:21 8:9,19 9:9,16 10:2,7 11:16 12:12,17 13:6 18:1,10 21:1, 7 22:14 23:2 24:2, 19,22 26:23 27:15 29:21 30:4,6,8,23 37:14 39:14 41:1 44:15 52:11 53:4, 20 54:1 57:13 60:13 62:2,15 65:7 69:5 72:5,9 73:12,17 76:2 78:19 79:8,11
threads 8:22 9:11,21	traffic's 37:25	typically 15:11	walkie-talkie 17:19,21	
Thursday 4:1	transcript 4:23, 24 79:13	U	WAN 20:12	
time 7:14 8:18 9:4 24:20 28:12 29:24 53:19 61:14	transiting 42:13	U.S. 5:22	wanted 32:12 35:4 38:22 70:21, 24	
today 4:19 5:19 8:20 16:8 69:6	transits 44:6	underlying 12:10	ways 13:16 26:20 61:18	
today's 4:23	transmission 43:9 45:21	understand 4:18 5:10,21 7:25 8:3 36:12	weaving 8:6,22	
told 51:20	transmitted 32:21,24 46:20 47:1,14 55:6 75:18,20 76:4,6	understanding 8:20 9:17,19 15:4, 7 16:1,6,9 26:8,11 32:8 42:10 50:20, 22 59:13 70:13	Web 78:6,18,21, 22 79:5	
top 14:1 25:9	transmitter 17:14 53:11	understood 5:15 6:16 7:14	well-known 7:8	Zoom 4:2
topic 28:8	transmitting 41:14,21 42:3 43:10,16 44:6,18 45:5,9,18 46:20 47:2,4,11,14 48:17 49:4,8 51:1, 4,6 53:3,7 75:2, 13,18,21 76:1,5 77:23	unquote 76:9	wide 20:12 23:10	
topology 7:19 10:8,9,15,20,23, 25 11:4 19:23 20:4 21:10,15,23 22:1,3,8,16,17,20 25:10 28:16 37:1 38:18 44:11		unregistered 46:18 75:19	wired 11:24	
totally 16:6		update 56:10,20	wireless 11:13, 14,17,20,25 12:20	
touch 69:17 70:19		updated 55:7 56:4	wirelessly 17:11, 13	
		uploading 24:23	word 7:8,9,10,24, 25 8:11 12:8 15:16 16:9 22:7 26:1 27:22 58:24	
		upstream 32:24 34:1,14	words 9:18 15:18	